

GS-4012F/4024

Intelligent Layer 3+ Switch

User's Guide

Version 3.8
6/2007
Edition 1

DEFAULT LOGIN

IP Address	http://192.168.1.1
User Name	admin
Password	1234



About This User's Guide

Intended Audience

This manual is intended for people who want to configure the GS-4024 or GS-4012F using the web configurator or via commands. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.



It is recommended you use the web configurator to configure the Switch.

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.
E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



Warnings tell you about things that could harm you or your device.








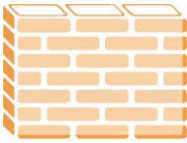



Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The GS-4024 and GS-4012F models may be referred to as the “Switch”, the “device”, the “system” or the “product” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings



For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- For continued protection against risk of fire replace only with same type and rating of fuse.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- The length of exposed (bare) power wire should not exceed 7mm.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction and Hardware	35
Getting to Know Your Switch	37
Hardware Installation and Connection	41
Hardware Overview	45
Basic Configuration	53
The Web Configurator	55
Initial Setup Example	65
System Status and Port Statistics	71
Basic Setting	77
Advanced	89
VLAN	91
Static MAC Forward Setup	105
Filtering	107
Spanning Tree Protocol	109
Bandwidth Control	127
Broadcast Storm Control	129
Mirroring	131
Link Aggregation	133
Port Authentication	141
Port Security	147
Classifier	151
Policy Rule	157
Queuing Method	163
VLAN Stacking	165
Multicast	171
Authentication & Accounting	185
IP Source Guard	199
Loop Guard	219
IP Application	223
Static Route	225
RIP	227
OSPF	229
IGMP	241
DVMRP	245

IP Multicast	249
Differentiated Services	251
DHCP	259
VRRP	267
Management, CLI, Troubleshooting	277
Maintenance	279
Access Control	285
Diagnostic	303
Syslog	305
Cluster Management	309
MAC Table	315
IP Table	317
ARP Table	319
Routing Table	321
Configure Clone	323
Introducing Commands	325
User and Enable Mode Commands	377
Configuration Mode Commands	383
Interface Commands	395
IEEE 802.1Q Tagged VLAN Commands	403
Multicast VLAN Registration Commands	411
Routing Domain Command Examples	413
Troubleshooting	415
Appendices and Index	423

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	25
List of Tables.....	31
Part I: Introduction and Hardware	35
Chapter 1	
Getting to Know Your Switch.....	37
1.1 Introduction	37
1.1.1 Backbone Application	37
1.1.2 Bridging Example	38
1.1.3 High Performance Switching Example	38
1.1.4 IEEE 802.1Q VLAN Application Examples	39
Chapter 2	
Hardware Installation and Connection	41
2.1 Freestanding Installation	41
2.2 Mounting the Switch on a Rack	42
2.2.1 Rack-mounted Installation Requirements	42
2.2.2 Attaching the Mounting Brackets to the Switch	42
2.2.3 Mounting the Switch on a Rack	43
Chapter 3	
Hardware Overview.....	45
3.1 Front Panel Connection	45
3.1.1 Console Port	46
3.1.2 Gigabit Ethernet Ports	46
3.1.3 SFP Slots	47
3.2 Rear Panel	48

3.3 Power Connections Overview	49
3.3.1 AC Power Connection	49
3.3.2 DC Power Connection	50
3.3.3 External Backup Power Supply Connector	51
3.3.4 Powering on the Switch	51
3.4 LEDs	51
 Part II: Basic Configuration.....	53
 Chapter 4	
The Web Configurator	55
4.1 Introduction	55
4.2 System Login	55
4.3 The Status Screen	56
4.3.1 Change Your Password	61
4.4 Saving Your Configuration	61
4.5 Switch Lockout	61
4.6 Resetting the Switch	62
4.6.1 Reload the Configuration File	62
4.7 Logging Out of the Web Configurator	63
4.8 Help	63
 Chapter 5	
Initial Setup Example.....	65
5.1 Overview	65
5.1.1 Configuring an IP Interface	65
5.1.2 Configuring DHCP Server Settings	66
5.1.3 Creating a VLAN	67
5.1.4 Setting Port VID	68
5.1.5 Enabling RIP	69
 Chapter 6	
System Status and Port Statistics.....	71
6.1 Overview	71
6.2 Port Status Summary	71
6.2.1 Status: Port Details	72
 Chapter 7	
Basic Setting	77
7.1 Overview	77
7.2 System Information	77

7.3 General Setup	79
7.4 Introduction to VLANs	81
7.5 Switch Setup Screen	81
7.6 IP Setup	83
7.6.1 IP Interfaces	83
7.7 Port Setup	85
 Part III: Advanced.....	 89
 Chapter 8	
VLAN	91
8.1 Introduction to IEEE 802.1Q Tagged VLANs	91
8.1.1 Forwarding Tagged and Untagged Frames	91
8.2 Automatic VLAN Registration	92
8.2.1 GARP	92
8.2.2 GVRP	92
8.3 Port VLAN Trunking	93
8.4 Select the VLAN Type	93
8.5 Static VLAN	93
8.5.1 Static VLAN Status	94
8.5.2 Static VLAN Details	94
8.5.3 Configure a Static VLAN	95
8.5.4 Configure VLAN Port Settings	96
8.6 Subnet Based VLANs	98
8.7 Configuring Subnet Based VLAN	99
8.8 Port-based VLAN Setup	100
8.8.1 Configure a Port-based VLAN	101
 Chapter 9	
Static MAC Forward Setup.....	105
9.1 Overview	105
9.2 Configuring Static MAC Forwarding	105
 Chapter 10	
Filtering.....	107
10.1 Configure a Filtering Rule	107
 Chapter 11	
Spanning Tree Protocol.....	109
11.1 STP/RSTP Overview	109
11.1.1 STP Terminology	109

11.1.2 How STP Works	110
11.1.3 STP Port States	111
11.1.4 Multiple RSTP	111
11.1.5 Multiple STP	112
11.2 Spanning Tree Protocol Status Screen	114
11.3 Spanning Tree Configuration	115
11.4 Configure Rapid Spanning Tree Protocol	116
11.5 Rapid Spanning Tree Protocol Status	117
11.6 Configure Multiple Rapid Spanning Tree Protocol	119
11.7 Multiple Rapid Spanning Tree Protocol Status	120
11.8 Configure Multiple Spanning Tree Protocol	122
11.9 Multiple Spanning Tree Protocol Status	124
Chapter 12	
Bandwidth Control.....	127
12.1 Bandwidth Control Overview	127
12.1.1 CIR and PIR	127
12.2 Bandwidth Control Setup	127
Chapter 13	
Broadcast Storm Control	129
13.1 Broadcast Storm Control Setup	129
Chapter 14	
Mirroring	131
14.1 Port Mirroring Setup	131
Chapter 15	
Link Aggregation	133
15.1 Link Aggregation Overview	133
15.2 Dynamic Link Aggregation	133
15.2.1 Link Aggregation ID	134
15.3 Link Aggregation Status	134
15.4 Link Aggregation Setting	135
15.5 Link Aggregation Control Protocol	136
15.6 Static Trunking Example	138
Chapter 16	
Port Authentication.....	141
16.1 Port Authentication Overview	141
16.1.1 IEEE 802.1x Authentication	141
16.1.2 MAC Authentication	142
16.2 Port Authentication Configuration	143

16.2.1 Activate IEEE 802.1x Security	143
16.2.2 Activate MAC Authentication	144
Chapter 17	
Port Security.....	147
17.1 About Port Security	147
17.2 Port Security Setup	147
Chapter 18	
Classifier.....	151
18.1 About the Classifier and QoS	151
18.2 Configuring the Classifier	151
18.3 Viewing and Editing Classifier Configuration	154
18.4 Classifier Example	155
Chapter 19	
Policy Rule.....	157
19.1 Policy Rules Overview	157
19.1.1 DiffServ	157
19.1.2 DSCP and Per-Hop Behavior	157
19.2 Configuring Policy Rules	158
19.3 Viewing and Editing Policy Configuration	160
19.4 Policy Example	161
Chapter 20	
Queuing Method.....	163
20.1 Queuing Method Overview	163
20.1.1 Strictly Priority Queuing	163
20.1.2 Weighted Round Robin Scheduling (WRR)	163
20.2 Configuring Queuing	164
Chapter 21	
VLAN Stacking	165
21.1 VLAN Stacking Overview	165
21.1.1 VLAN Stacking Example	165
21.2 VLAN Stacking Port Roles	166
21.3 VLAN Tag Format	167
21.3.1 Frame Format	167
21.4 Configuring VLAN Stacking	168
Chapter 22	
Multicast	171
22.1 Multicast Overview	171

22.1.1 IP Multicast Addresses	171
22.1.2 IGMP Filtering	171
22.1.3 IGMP Snooping	171
22.1.4 IGMP Snooping and VLANs	172
22.2 Multicast Status	172
22.3 Multicast Setting	172
22.4 IGMP Snooping VLAN	174
22.5 IGMP Filtering Profile	176
22.6 MVR Overview	177
22.6.1 Types of MVR Ports	177
22.6.2 MVR Modes	178
22.6.3 How MVR Works	178
22.7 General MVR Configuration	178
22.8 MVR Group Configuration	180
22.8.1 MVR Configuration Example	181
 Chapter 23	
Authentication & Accounting	185
23.1 Authentication, Authorization and Accounting	185
23.1.1 Local User Accounts	185
23.1.2 RADIUS and TACACS+	186
23.2 Authentication and Accounting Screens	186
23.2.1 RADIUS Server Setup	186
23.2.2 TACACS+ Server Setup	188
23.2.3 Authentication and Accounting Setup	190
23.2.4 Vendor Specific Attribute	193
23.3 Supported RADIUS Attributes	194
23.3.1 Attributes Used for Authentication	195
23.3.2 Attributes Used for Accounting	195
 Chapter 24	
IP Source Guard.....	199
24.1 IP Source Guard Overview	199
24.1.1 DHCP Snooping Overview	199
24.1.2 ARP Inspection Overview	201
24.2 IP Source Guard	203
24.3 IP Source Guard Static Binding	203
24.4 DHCP Snooping	205
24.5 DHCP Snooping Configure	208
24.5.1 DHCP Snooping Port Configure	209
24.5.2 DHCP Snooping VLAN Configure	211
24.6 ARP Inspection Status	212
24.6.1 ARP Inspection VLAN Status	212

24.6.2 ARP Inspection Log Status	213
24.7 ARP Inspection Configure	215
24.7.1 ARP Inspection Port Configure	216
24.7.2 ARP Inspection VLAN Configure	217
Chapter 25	
Loop Guard.....	219
25.1 Loop Guard Overview	219
25.2 Loop Guard Setup	221
 Part IV: IP Application.....	 223
Chapter 26	
Static Route	225
26.1 Configuring Static Routing	225
Chapter 27	
RIP	227
27.1 RIP Overview	227
27.2 Configuring RIP	227
Chapter 28	
OSPF	229
28.1 OSPF Overview	229
28.1.1 OSPF Autonomous Systems and Areas	229
28.1.2 How OSPF Works	230
28.1.3 Interfaces and Virtual Links	230
28.1.4 OSPF and Router Elections	230
28.1.5 Configuring OSPF	231
28.2 OSPF Status	231
28.3 OSPF Configuration	233
28.4 Configure OSPF Areas	235
28.4.1 View OSPF Area Information Table	236
28.5 Configuring OSPF Interfaces	236
28.6 OSPF Virtual-Links	238
Chapter 29	
IGMP.....	241
29.1 IGMP Overview	241
29.1.1 How IGMP Works	242
29.2 Port-based IGMP	243

29.3 Configuring IGMP	243
Chapter 30	
DVMRP	245
30.1 DVMRP Overview	245
30.2 How DVMRP Works	245
30.2.1 DVMRP Terminology	246
30.3 Configuring DVMRP	246
30.3.1 DVMRP Configuration Error Messages	247
30.4 Default DVMRP Timer Values	248
Chapter 31	
IP Multicast	249
31.1 IP Multicast Overview	249
31.2 Configuring Multicast	249
Chapter 32	
Differentiated Services	251
32.1 DiffServ Overview	251
32.1.1 DSCP and Per-Hop Behavior	251
32.1.2 DiffServ Network Example	252
32.2 Two Rate Three Color Marker Traffic Policing	252
32.2.1 TRTCM - Color-blind Mode	253
32.2.2 TRTCM - Color-aware Mode	253
32.3 Activating DiffServ	254
32.3.1 Configuring 2-Rate 3 Color Marker Settings	254
32.4 DSCP-to-IEEE 802.1p Priority Settings	256
32.4.1 Configuring DSCP Settings	256
Chapter 33	
DHCP	259
33.1 DHCP Overview	259
33.1.1 DHCP Modes	259
33.1.2 DHCP Configuration Options	259
33.2 DHCP Status	260
33.3 DHCP Server Status Detail	260
33.4 DHCP Relay	261
33.4.1 DHCP Relay Agent Information	261
33.4.2 Configuring DHCP Global Relay	262
33.4.3 Global DHCP Relay Configuration Example	263
33.5 Configuring DHCP VLAN Settings	264
33.5.1 Example: DHCP Relay for Two VLANs	266

Chapter 34	
VRRP	267
34.1 VRRP Overview	267
34.2 VRRP Status	268
34.3 VRRP Configuration	269
34.3.1 IP Interface Setup	269
34.3.2 VRRP Parameters	270
34.3.3 Configuring VRRP Parameters	271
34.4 VRRP Configuration Summary	272
34.5 VRRP Configuration Examples	272
34.5.1 One Subnet Network Example	272
34.5.2 Two Subnets Example	274
 Part V: Management, CLI, Troubleshooting.....	 277
 Chapter 35	
Maintenance	279
35.1 The Maintenance Screen	279
35.2 Load Factory Default	280
35.3 Save Configuration	280
35.4 Reboot System	281
35.5 Firmware Upgrade	281
35.6 Restore a Configuration File	282
35.7 Backup a Configuration File	282
35.8 FTP Command Line	283
35.8.1 Filename Conventions	283
35.8.2 FTP Command Line Procedure	283
35.8.3 GUI-based FTP Clients	284
35.8.4 FTP Restrictions	284
 Chapter 36	
Access Control.....	285
36.1 Access Control Overview	285
36.2 The Access Control Main Screen	285
36.3 About SNMP	286
36.3.1 SNMP v3 and Security	287
36.3.2 Supported MIBs	287
36.3.3 SNMP Traps	287
36.3.4 Configuring SNMP	291
36.3.5 Configuring SNMP Trap Group	293
36.3.6 Setting Up Login Accounts	294

36.4 SSH Overview	296
36.5 How SSH works	296
36.6 SSH Implementation on the Switch	297
36.6.1 Requirements for Using SSH	297
36.7 Introduction to HTTPS	297
36.8 HTTPS Example	298
36.8.1 Internet Explorer Warning Messages	298
36.8.2 Netscape Navigator Warning Messages	299
36.8.3 The Main Screen	299
36.9 Service Port Access Control	300
36.10 Remote Management	301
 Chapter 37	
Diagnostic.....	303
37.1 Diagnostic	303
 Chapter 38	
Syslog	305
38.1 Syslog Overview	305
38.2 Syslog Setup	305
38.3 Syslog Server Setup	306
 Chapter 39	
Cluster Management.....	309
39.1 Cluster Management Status Overview	309
39.2 Cluster Management Status	310
39.2.1 Cluster Member Switch Management	311
39.3 Clustering Management Configuration	312
 Chapter 40	
MAC Table.....	315
40.1 MAC Table Overview	315
40.2 Viewing the MAC Table	316
 Chapter 41	
IP Table	317
41.1 IP Table Overview	317
41.2 Viewing the IP Table	318
 Chapter 42	
ARP Table	319
42.1 ARP Table Overview	319
42.1.1 How ARP Works	319

42.2 Viewing the ARP Table	319
Chapter 43	
Routing Table	321
43.1 Overview	321
43.2 Viewing the Routing Table	321
Chapter 44	
Configure Clone	323
44.1 Configure Clone	323
Chapter 45	
Introducing Commands.....	325
45.1 Overview	325
45.2 Accessing the CLI	325
45.2.1 The Console Port	325
45.3 The Login Screen	326
45.4 Command Syntax Conventions	326
45.5 Changing the Password	327
45.6 Creating a New IP Interface	327
45.7 Privilege Levels	328
45.8 Command Modes	328
45.9 Getting Help	329
45.9.1 List of Available Commands	330
45.10 Using Command History	331
45.11 Saving Your Configuration	331
45.11.1 Switch Configuration File	332
45.11.2 Logging Out	332
45.12 Command Summary	332
45.12.1 User Mode	333
45.12.2 Enable Mode	334
45.12.3 General Configuration Mode	343
45.12.4 interface port-channel Commands	368
45.12.5 interface route-domain Commands	373
45.12.6 config-vlan Commands	375
45.13 mvr Commands	376
Chapter 46	
User and Enable Mode Commands.....	377
46.1 Overview	377
46.2 show Commands	377
46.2.1 show system-information	377
46.2.2 show ip	378

46.2.3 show logging	378
46.2.4 show interface	378
46.2.5 show mac address-table	379
46.3 ping	380
46.4 traceroute	380
46.5 Copy Port Attributes	381
46.6 Configuration File Maintenance	381
46.6.1 Using a Different Configuration File	382
46.6.2 Resetting to the Factory Default	382
Chapter 47	
Configuration Mode Commands	383
47.1 Change the Out of Band Management IP Address	383
47.2 Enabling IGMP Snooping	383
47.3 Configure IGMP Filter	384
47.4 Enabling STP	385
47.5 no Command Examples	387
47.5.1 Disable Commands	387
47.5.2 Resetting Commands	387
47.5.3 Re-enable commands	387
47.5.4 Other Examples of no Commands	388
47.6 Static Route Commands	390
47.7 Enabling MAC Filtering	390
47.8 Enabling Trunking	391
47.9 Enabling Port Authentication	392
47.9.1 RADIUS Server Settings	392
47.9.2 Port Authentication Settings	393
Chapter 48	
Interface Commands	395
48.1 Overview	395
48.2 Interface Command Examples	395
48.2.1 interface port-channel	395
48.2.2 bpdu-control	395
48.2.3 broadcast-limit	396
48.2.4 bandwidth-limit	396
48.2.5 mirror	397
48.2.6 gvrp	398
48.2.7 ingress-check	398
48.2.8 frame-type	398
48.2.9 weight	399
48.2.10 egress set	399
48.2.11 qos priority	400

48.2.12 name	400
48.2.13 speed-duplex	400
48.2.14 test	401
48.3 Interface no Command Examples	401
48.3.1 no bandwidth-limit	401
Chapter 49	
IEEE 802.1Q Tagged VLAN Commands	403
49.1 Configuring Tagged VLAN	403
49.2 Global VLAN1Q Tagged VLAN Configuration Commands	404
49.2.1 GARP Status	404
49.2.2 GARP Timer	404
49.2.3 GVRP Timer	405
49.2.4 Enable GVRP	405
49.2.5 Disable GVRP	405
49.3 Port VLAN Commands	405
49.3.1 Set Port VID	405
49.3.2 Set Acceptable Frame Type	406
49.3.3 Enable or Disable Port GVRP	406
49.3.4 Modify Static VLAN	406
49.3.5 Delete VLAN ID	408
49.4 Enable VLAN	408
49.5 Disable VLAN	408
49.6 Show VLAN Setting	408
Chapter 50	
Multicast VLAN Registration Commands	411
50.1 Overview	411
50.2 Create Multicast VLAN	411
Chapter 51	
Routing Domain Command Examples	413
51.0.1 interface route-domain	413
Chapter 52	
Troubleshooting	415
52.1 Problems Starting Up the Switch	415
52.2 Problems Accessing the Switch	415
52.2.1 Pop-up Windows, JavaScripts and Java Permissions	416
52.3 Problems with the Password	421
Part VI: Appendices and Index	423

Appendix A Product Specifications.....	425
Appendix B IP Addresses and Subnetting	431
Appendix C Common Services	441
Appendix D Legal Information	445
Appendix E Customer Support.....	449
Index.....	453

List of Figures

Figure 1 Backbone Application	38
Figure 2 Bridging Application	38
Figure 3 High Performance Switched Workgroup Application	39
Figure 4 Shared Server Using VLAN Example	40
Figure 5 Attaching Rubber Feet	41
Figure 6 Attaching the Mounting Brackets	43
Figure 7 Mounting the Switch on a Rack	43
Figure 8 Front Panel: GS-4024	45
Figure 9 Front Panel: GS-4012F	45
Figure 10 Transceiver Installation Example	47
Figure 11 Installed Transceiver	48
Figure 12 Opening the Transceiver's Latch Example	48
Figure 13 Transceiver Removal Example	48
Figure 14 Rear Panel: GS-4012F	48
Figure 15 Rear Panel: GS-4024	49
Figure 16 Rear Panel: GS-4012F (DC Model)	49
Figure 17 Rear Panel: GS-4024 (DC Model)	49
Figure 18 Terminal Block Pairs	50
Figure 19 Web Configurator: Login	56
Figure 20 Web Configurator Home Screen (Status)	56
Figure 21 Change Administrator Login Password	61
Figure 22 Resetting the Switch: Via the Console Port	63
Figure 23 Web Configurator: Logout Screen	63
Figure 24 Initial Setup Network Example: IP Interface	65
Figure 25 Initial Setup Network Example: VLAN	67
Figure 26 Initial Setup Network Example: Port VID	68
Figure 27 Status	71
Figure 28 Status > Port Details	73
Figure 29 System Info	78
Figure 30 Basic Setting > General Setup	79
Figure 31 Basic Setting > Switch Setup	82
Figure 32 Basic Setting > IP Setup	84
Figure 33 Basic Setting > Port Setup	86
Figure 34 Port VLAN Trunking	93
Figure 35 Switch Setup: Select VLAN Type	93
Figure 36 Advanced Application > VLAN: VLAN Status	94
Figure 37 Advanced Application > VLAN > VLAN Detail	94
Figure 38 Advanced Application > VLAN > Static VLAN	95

Figure 39 Advanced Application > VLAN > VLAN Port Setting	97
Figure 40 Subnet Based VLAN Application Example	98
Figure 41 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN	99
Figure 42 Port Based VLAN Setup (All Connected)	101
Figure 43 Port Based VLAN Setup (Port Isolation)	102
Figure 44 Advanced Application > Static MAC Forwarding	105
Figure 45 Advanced Application > Filtering	107
Figure 46 MRSTP Network Example	111
Figure 47 STP/RSTP Network Example	112
Figure 48 MSTP Network Example	113
Figure 49 MSTIs in Different Regions	114
Figure 50 MSTP and Legacy RSTP Network Example	114
Figure 51 Advanced Application > Spanning Tree Protocol	115
Figure 52 Advanced Application > Spanning Tree Protocol > Configuration	115
Figure 53 Advanced Application > Spanning Tree Protocol > RSTP	116
Figure 54 Advanced Application > Spanning Tree Protocol > Status: RSTP	118
Figure 55 Advanced Application > Spanning Tree Protocol > MRSTP	119
Figure 56 Advanced Application > Spanning Tree Protocol > Status: MRSTP	121
Figure 57 Advanced Application > Spanning Tree Protocol > MSTP	122
Figure 58 Advanced Application > Spanning Tree Protocol > Status: MSTP	125
Figure 59 Advanced Application > Bandwidth Control	128
Figure 60 Advanced Application > Broadcast Storm Control	129
Figure 61 Advanced Application > Mirroring	131
Figure 62 Advanced Application > Link Aggregation Status	134
Figure 63 Advanced Application > Link Aggregation > Link Aggregation Setting	135
Figure 64 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP	137
Figure 65 Trunking Example - Physical Connections	138
Figure 66 Trunking Example - Configuration Screen	139
Figure 67 IEEE 802.1x Authentication Process	142
Figure 68 MAC Authentication Process	142
Figure 69 Advanced Application > Port Authentication	143
Figure 70 Advanced Application > Port Authentication > 802.1x	143
Figure 71 Advanced Application > Port Authentication > MAC Authentication	145
Figure 72 Advanced Application > Port Security	148
Figure 73 Advanced Application > Classifier	152
Figure 74 Advanced Application > Classifier: Summary Table	154
Figure 75 Classifier: Example	156
Figure 76 Advanced Application > Policy Rule	158
Figure 77 Advanced Application > Policy Rule: Summary Table	160
Figure 78 Policy Example	161
Figure 79 Queuing Method	164
Figure 80 VLAN Stacking Example	166
Figure 81 Advanced Application > VLAN Stacking	168

Figure 82 Advanced Application > Multicast	172
Figure 83 Advanced Application > Multicast > Multicast Setting	173
Figure 84 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN	175
Figure 85 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile	176
Figure 86 MVR Network Example	177
Figure 87 MVR Multicast Television Example	178
Figure 88 Advanced Application > Multicast > Multicast Setting > MVR	179
Figure 89 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration	181
Figure 90 MVR Configuration Example	182
Figure 91 MVR Configuration Example	182
Figure 92 MVR Group Configuration Example	182
Figure 93 MVR Group Configuration Example	183
Figure 94 AAA Server	185
Figure 95 Advanced Application > Auth and Acct	186
Figure 96 Advanced Application > Auth and Acct > RADIUS Server Setup	187
Figure 97 Advanced Application > Auth and Acct > TACACS+ Server Setup	189
Figure 98 Advanced Application > Auth and Acct > Auth and Acct Setup	191
Figure 99 DHCP Snooping Database File Format	200
Figure 100 Example: Man-in-the-middle Attack	201
Figure 101 IP Source Guard	203
Figure 102 IP Source Guard Static Binding	204
Figure 103 DHCP Snooping	205
Figure 104 DHCP Snooping Configure	208
Figure 105 DHCP Snooping Port Configure	210
Figure 106 DHCP Snooping VLAN Configure	211
Figure 107 ARP Inspection Status	212
Figure 108 ARP Inspection VLAN Status	213
Figure 109 ARP Inspection Log Status	214
Figure 110 ARP Inspection Configure	215
Figure 111 ARP Inspection Port Configure	216
Figure 112 ARP Inspection VLAN Configure	217
Figure 113 Loop Guard vs STP	219
Figure 114 Switch in Loop State	220
Figure 115 Loop Guard - Probe Packet	220
Figure 116 Loop Guard - Network Loop	220
Figure 117 Advanced Application > Loop Guard	221
Figure 118 Static Routing	225
Figure 119 RIP	228
Figure 120 OSPF Network Example	230
Figure 121 OSPF Router Election Example	231
Figure 122 OSPF Status	232
Figure 123 OSPF Configuration: Area Setup	235
Figure 124 OSPF Configuration: Summary Table	236

Figure 125 OSPF Interface	237
Figure 126 OSPF Virtual Link	238
Figure 127 IP Multicast	241
Figure 128 IGMP Version 1 Example	242
Figure 129 IGMP Version 2 Example	242
Figure 130 IGMP Version 3 Example	243
Figure 131 IP Application > IGMP	243
Figure 132 How DVMRP Works	246
Figure 133 DVMRP	246
Figure 134 DVMRP: IGMP/RIP Not Set Error	247
Figure 135 DVMRP: Unable to Disable IGMP Error	247
Figure 136 DVMRP: Duplicate VID Error Message	247
Figure 137 IP Multicast	249
Figure 138 DiffServ: Differentiated Service Field	251
Figure 139 DiffServ Network	252
Figure 140 TRTCM - Color-blind Mode	253
Figure 141 TRTCM - Color-aware Mode	253
Figure 142 IP Application > DiffServ	254
Figure 143 IP Application > DiffServ > 2-rate 3 Color Marker	255
Figure 144 IP Application > DiffServ > DSCP Setting	256
Figure 145 IP Application > DHCP Status	260
Figure 146 IP Application > DHCP > DHCP Server Status Detail	260
Figure 147 IP Application > DHCP > Global	262
Figure 148 Global DHCP Relay Network Example	263
Figure 149 DHCP Relay Configuration Example	263
Figure 150 IP Application > DHCP > VLAN	264
Figure 151 DHCP Relay for Two VLANs	266
Figure 152 DHCP Relay for Two VLANs Configuration Example	266
Figure 153 VRRP: Example 1	267
Figure 154 VRRP Status	268
Figure 155 VRRP Configuration: IP Interface	269
Figure 156 VRRP Configuration: VRRP Parameters	271
Figure 157 VRRP Configuration: Summary	272
Figure 158 VRRP Configuration Example: One Virtual Router Network	273
Figure 159 VRRP Example 1: VRRP Parameter Settings on Switch A	273
Figure 160 VRRP Example 1: VRRP Parameter Settings on Switch B	273
Figure 161 VRRP Example 1: VRRP Status on Switch A	273
Figure 162 VRRP Example 1: VRRP Status on Switch B	274
Figure 163 VRRP Configuration Example: Two Virtual Router Network	274
Figure 164 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A	274
Figure 165 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B	275
Figure 166 VRRP Example 2: VRRP Status on Switch A	275
Figure 167 VRRP Example 2: VRRP Status on Switch B	275

Figure 168 Maintenance	279
Figure 169 Load Factory Default: Start	280
Figure 170 Reboot System: Confirmation	281
Figure 171 Firmware Upgrade	281
Figure 172 Restore Configuration	282
Figure 173 Backup Configuration	282
Figure 174 Access Control	285
Figure 175 SNMP Management Model	286
Figure 176 Access Control: SNMP	292
Figure 177 Access Control: SNMP: Trap Group	294
Figure 178 Access Control: Logins	295
Figure 179 SSH Communication Example	296
Figure 180 How SSH Works	296
Figure 181 HTTPS Implementation	298
Figure 182 Security Alert Dialog Box (Internet Explorer)	298
Figure 183 Security Certificate 1 (Netscape)	299
Figure 184 Security Certificate 2 (Netscape)	299
Figure 185 Example: Lock Denoting a Secure Connection	300
Figure 186 Access Control: Service Access Control	300
Figure 187 Access Control: Remote Management	301
Figure 188 Diagnostic	303
Figure 189 Syslog	306
Figure 190 Syslog: Server Setup	307
Figure 191 Clustering Application Example	310
Figure 192 Cluster Management: Status	310
Cluster Management: Cluster Member Web Configurator Screen	311
Example: Uploading Firmware to a Cluster Member Switch	312
Figure 195 Clustering Management Configuration	313
Figure 196 MAC Table Flowchart	315
Figure 197 MAC Table	316
Figure 198 IP Table Flowchart	317
Figure 199 IP Table	318
Figure 200 ARP Table	320
Figure 201 Routing Table Status	321
Figure 202 Configure Clone	323
Figure 203 no port-access-authenticator Command Example	389
Figure 204 Pop-up Blocker	416
Figure 205 Internet Options	417
Figure 206 Internet Options	418
Figure 207 Pop-up Blocker Settings	418
Figure 208 Internet Options	419
Figure 209 Security Settings - Java Scripting	420
Figure 210 Security Settings - Java	420

Figure 211 Java (Sun)	421
Figure 212 Network Number and Host ID	432
Figure 213 Subnetting Example: Before Subnetting	434
Figure 214 Subnetting Example: After Subnetting	435
Figure 215 Conflicting Computer IP Addresses Example	439
Figure 216 Conflicting Computer IP Addresses Example	439
Figure 217 Conflicting Computer and Router IP Addresses Example	440

List of Tables

Table 1 Front Panel	45
Table 2 LEDs	51
Table 3 Navigation Panel Sub-links Overview	57
Table 4 Web Configurator Screen Sub-links Details	58
Table 5 Navigation Panel Links	59
Table 6 Status	71
Table 7 Status: Port Details	73
Table 8 System Info	78
Table 9 Basic Setting > General Setup	80
Table 10 Basic Setting > Switch Setup	82
Table 11 Basic Setting > IP Setup	84
Table 12 Basic Setting > Port Setup	86
Table 13 IEEE 802.1Q VLAN Terminology	92
Table 14 Advanced Application > VLAN: VLAN Status	94
Table 15 Advanced Application > VLAN > VLAN Detail	95
Table 16 Advanced Application > VLAN > Static VLAN	96
Table 17 Advanced Application > VLAN > VLAN Port Setting	97
Table 18 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup	99
Table 19 Port Based VLAN Setup	102
Table 20 Advanced Application > Static MAC Forwarding	106
Table 21 Advanced Application > Filtering	107
Table 22 STP Path Costs	110
Table 23 STP Port States	111
Table 24 Advanced Application > Spanning Tree Protocol > Configuration	115
Table 25 Advanced Application > Spanning Tree Protocol > RSTP	116
Table 26 Advanced Application > Spanning Tree Protocol > Status: RSTP	118
Table 27 Advanced Application > Spanning Tree Protocol > MRSTP	119
Table 28 Advanced Application > Spanning Tree Protocol > Status: MRSTP	121
Table 29 Advanced Application > Spanning Tree Protocol > MSTP	123
Table 30 Advanced Application > Spanning Tree Protocol > Status: MSTP	125
Table 31 Advanced Application > Bandwidth Control	128
Table 32 Advanced Application > Broadcast Storm Control	130
Table 33 Advanced Application > Mirroring	132
Table 34 Link Aggregation ID: Local Switch	134
Table 35 Link Aggregation ID: Peer Switch	134
Table 36 Advanced Application > Link Aggregation Status	134
Table 37 Advanced Application > Link Aggregation > Link Aggregation Setting	136
Table 38 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP	137

Table 39 Advanced Application > Port Authentication > 802.1x	144
Table 40 Advanced Application > Port Authentication > MAC Authentication	145
Table 41 Advanced Application > Port Security	148
Table 42 Advanced Application > Classifier	152
Table 43 Classifier: Summary Table	154
Table 44 Common Ethernet Types and Protocol Number	154
Table 45 Common IP Ports	155
Table 46 Advanced Application > Policy Rule	159
Table 47 Advanced Application > Policy Rule: Summary Table	160
Table 48 Queuing Method	164
Table 49 VLAN Tag Format	167
Table 50 Single and Double Tagged 802.11Q Frame Format	167
Table 51 802.1Q Frame	167
Table 52 Advanced Application > VLAN Stacking	168
Table 53 Multicast Status	172
Table 54 Advanced Application > Multicast > Multicast Setting	173
Table 55 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN	175
Table 56 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile	176
Table 57 Advanced Application > Multicast > Multicast Setting > MVR	179
Table 58 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration	181
Table 59 RADIUS vs TACACS+	186
Table 60 Advanced Application > Auth and Acct > RADIUS Server Setup	187
Table 61 Advanced Application > Auth and Acct > TACACS+ Server Setup	189
Table 62 Advanced Application > Auth and Acct > Auth and Acct Setup	191
Table 63 Supported VSAs	193
Table 64 Supported Tunnel Protocol Attribute	194
Table 65 RADIUS Attributes - Exec Events via Console	196
Table 66 RADIUS Attributes - Exec Events via Telnet/SSH	196
Table 67 RADIUS Attributes - Exec Events via Console	196
Table 68 IP Source Guard	203
Table 69 IP Source Guard Static Binding	204
Table 70 DHCP Snooping	206
Table 71 DHCP Snooping Configure	208
Table 72 DHCP Snooping Port Configure	210
Table 73 DHCP Snooping VLAN Configure	211
Table 74 ARP Inspection Status	212
Table 75 ARP Inspection VLAN Status	213
Table 76 ARP Inspection Log Status	214
Table 77 ARP Inspection Configure	215
Table 78 ARP Inspection Port Configure	217
Table 79 ARP Inspection VLAN Configure	218
Table 80 Advanced Application > Loop Guard	221
Table 81 Static Routing	225

Table 82 RIP	228
Table 83 OSPF vs. RIP	229
Table 84 OSPF: Router Types	229
Table 85 OSPF Status	232
Table 86 OSPF Status: Common Output Fields	232
Table 87 OSPF Configuration: Activating and General Settings	234
Table 88 OSPF Configuration: Area Setup	235
Table 89 OSPF Configuration: Summary Table	236
Table 90 OSPF Interface	237
Table 91 OSPF Virtual-Link	239
Table 92 IP Application > IGMP	244
Table 93 DVMRP	246
Table 94 DVMRP: Default Timer Values	248
Table 95 IP Multicast	250
Table 96 IP Application > DiffServ	254
Table 97 IP Application > DiffServ > 2-rate 3 Color Marker	255
Table 98 Default DSCP-IEEE 802.1p Mapping	256
Table 99 IP Application > DiffServ > DSCP Setting	257
Table 100 IP Application > DHCP Status	260
Table 101 IP Application > DHCP Server Status Detail	261
Table 102 Relay Agent Information	262
Table 103 IP Application > DHCP > Global	262
Table 104 IP Application > DHCP > VLAN	265
Table 105 VRRP Status	268
Table 106 VRRP Configuration: IP Interface	270
Table 107 VRRP Configuration: VRRP Parameters	271
Table 108 VRRP Configuring: VRRP Parameters	272
Table 109 Maintenance	279
Table 110 Filename Conventions	283
Table 111 Access Control Overview	285
Table 112 SNMP Commands	286
Table 113 SNMP System Traps	287
Table 114 SNMP InterfaceTraps	289
Table 115 AAA Traps	289
Table 116 SNMP IP Traps	290
Table 117 SNMP Switch Traps	291
Table 118 Access Control: SNMP	292
Table 119 Access Control: SNMP: Trap Group	294
Table 120 Access Control: Logins	295
Table 121 Access Control: Service Access Control	301
Table 122 Access Control: Remote Management	301
Table 123 Diagnostic	303
Table 124 Syslog Severity Levels	305

Table 125 Syslog	306
Table 126 Syslog: Server Setup	307
Table 127 ZyXEL Clustering Management Specifications	309
Table 128 Cluster Management: Status	311
Table 129 FTP Upload to Cluster Member Example	312
Table 130 Clustering Management Configuration	313
Table 131 MAC Table	316
Table 132 IP Table	318
Table 133 ARP Table	320
Table 134 Routing Table Status	321
Table 135 Configure Clone	324
Table 136 Command Interpreter Mode Summary	329
Table 137 Command Summary: User Mode	333
Table 138 Command Summary: Enable Mode	334
Table 139 Command Summary: Configuration Mode	343
Table 140 interface port-channel Commands	368
Table 141 interface route-domain Commands	373
Table 142 Command Summary: config-vlan Commands	375
Table 143 Command Summary: mvr Commands	376
Table 144 Troubleshooting the Start-Up of Your Switch	415
Table 145 Troubleshooting Accessing the Switch	415
Table 146 Troubleshooting the Password	421
Table 147 Hardware Specifications	425
Table 148 Firmware Specifications	426
Table 149 Feature Specifications	428
Table 150 Standards Supported	429
Table 151 IP Address Network Number and Host ID Example	432
Table 152 Subnet Masks	433
Table 153 Maximum Host Numbers	433
Table 154 Alternative Subnet Mask Notation	433
Table 155 Subnet 1	435
Table 156 Subnet 2	436
Table 157 Subnet 3	436
Table 158 Subnet 4	436
Table 159 Eight Subnets	436
Table 160 24-bit Network Number Subnet Planning	437
Table 161 16-bit Network Number Subnet Planning	437
Table 162 Commonly Used Services	441

PART I

Introduction and Hardware

Getting to Know Your Switch (37)

Hardware Installation and Connection (41)

Hardware Overview (45)

Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

1.1 Introduction

Your Switch is a stand-alone layer-3 Gigabit Ethernet switch. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The GS-4024 is a stand-alone layer 3 Ethernet switch with 20 Gigabit Ethernet ports and 4 GbE dual personality interfaces for uplink. A dual personality interface includes one Gigabit port and one slot for mini-GBIC transceiver (SFP module) with one port active at a time.

The GS-4012F comes with 8 min-GBIC slots and 4 GbE dual personality interfaces for uplink. There are two GS-4012F models. The GS-4012F DC model requires DC power supply input of -48 VDC to -60 VDC, 1.5A Max no tolerance. The GS-4012F AC model requires 100~240VAC, 1.6A power.

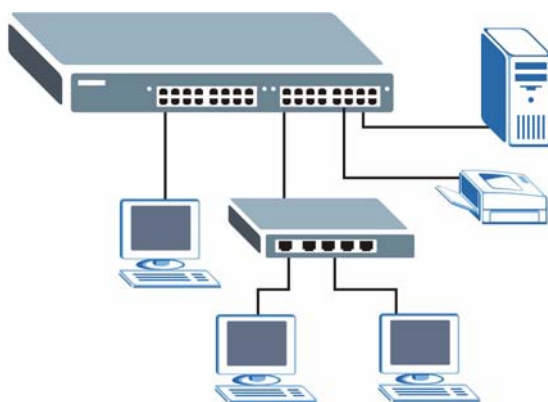
With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See [Appendix A on page 425](#) for a full list of software features available on the Switch.

1.1.1 Backbone Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

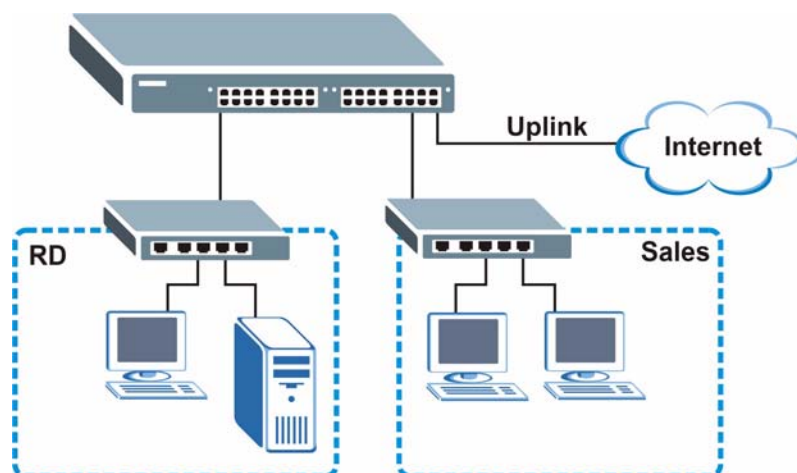
In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application

1.1.2 Bridging Example

In this example application the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

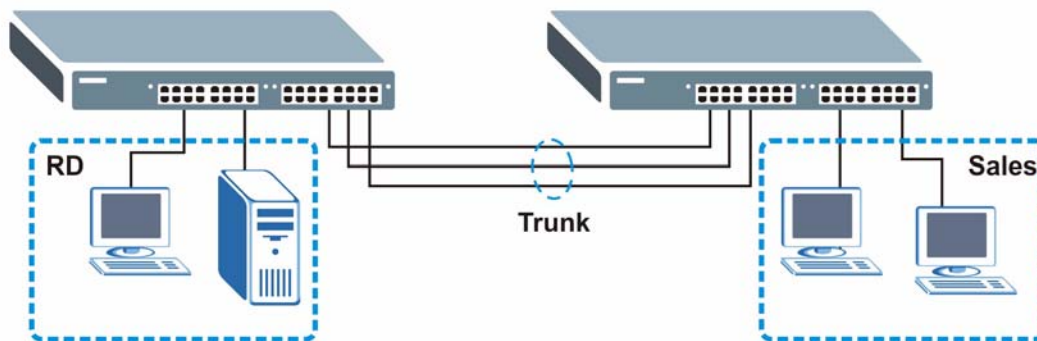
Figure 2 Bridging Application

1.1.3 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

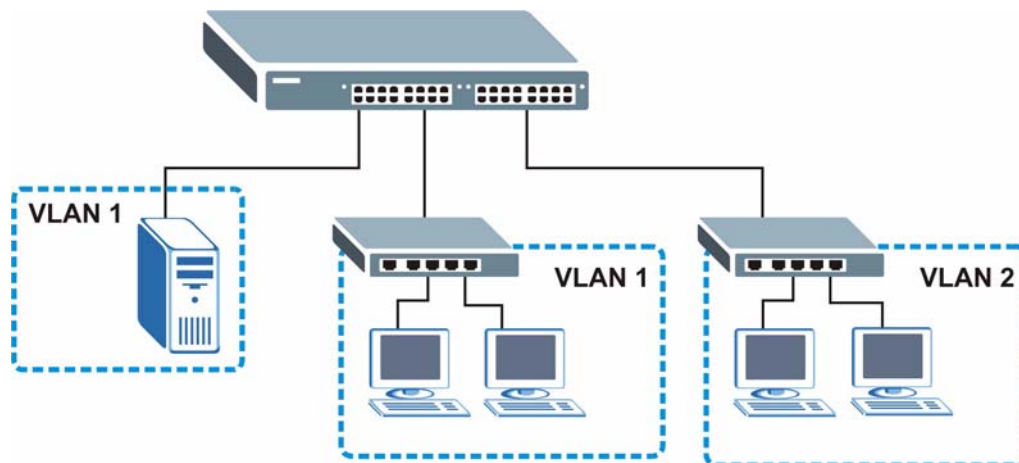
For more information on VLANs, refer to [Chapter 8 on page 91](#).

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



Hardware Installation and Connection

This chapter shows you how to install the hardware and make port connections.

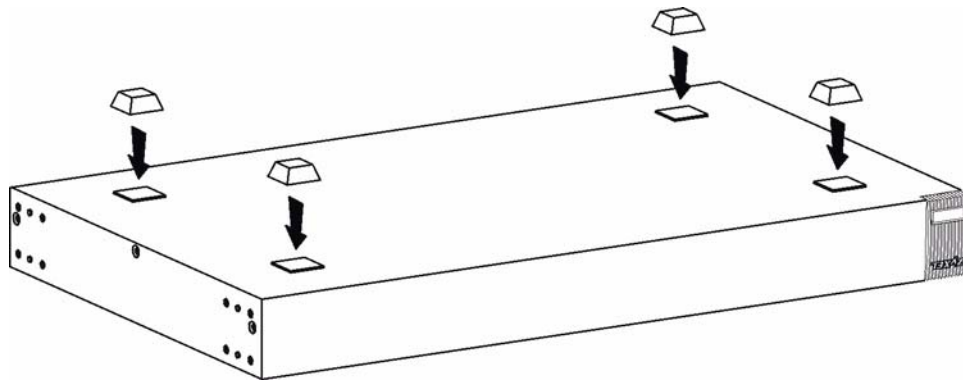


Example graphics are shown.

2.1 Freestanding Installation

- 1 Make sure the Switch is clean and dry.
- 2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.
- 4 Remove the adhesive backing from the rubber feet.
- 5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 5 Attaching Rubber Feet





Do NOT block the ventilation holes. Leave space between devices when stacking.



For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.



Make sure that no objects obstruct the airflow of the fans.

2.2.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.



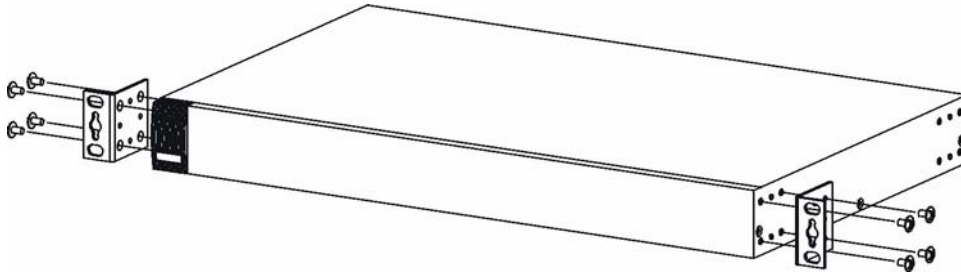
Failure to use the proper screws may damage the unit.

2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.2 Attaching the Mounting Brackets to the Switch

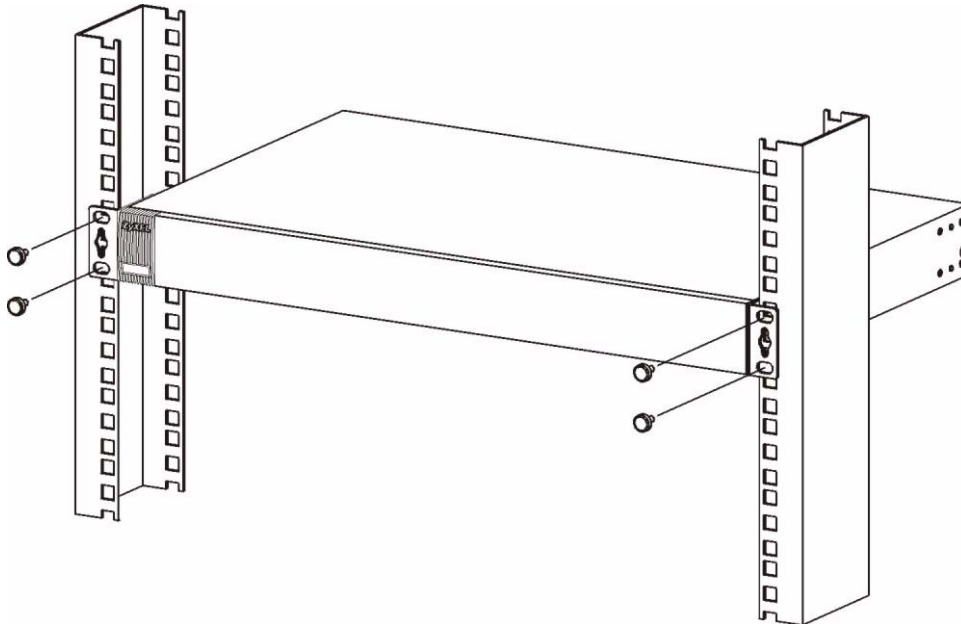
- 1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 6 Attaching the Mounting Brackets

- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

- 1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 7 Mounting the Switch on a Rack

- 2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

Hardware Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel Connection

The figure below shows the front panel of the Switch.

Figure 8 Front Panel: GS-4024

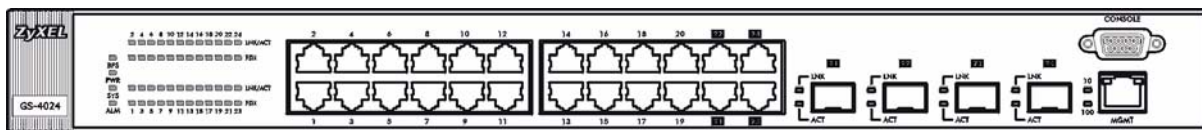
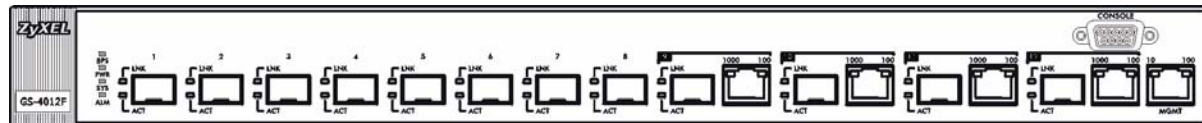


Figure 9 Front Panel: GS-4012F



The following table describes the port labels on the front panel.

Table 1 Front Panel

PORT	DESCRIPTION
MGMT	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.
CONSOLE	Only connect this port if you want to configure the Switch using the command line interface (CLI) via the console port.
GS-4024 Model	
20 100/1000 Mbps RJ-45 Gigabit Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.

Table 1 Front Panel (continued)

PORT	DESCRIPTION
Four Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.
	<ul style="list-style-type: none"> 4 100/1000 Mbps RJ-45 Gigabit Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.
	<ul style="list-style-type: none"> 4 Mini-GBIC Ports: Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches (see Section 3.1.3 on page 47 for instructions).
GS-4012F Model	
8 Mini-GBIC Slots	Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches (see Section 3.1.3 on page 47 for instructions).
Four Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.
	<ul style="list-style-type: none"> 4 100/1000 Mbps RJ-45 Gigabit Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.
	<ul style="list-style-type: none"> 4 Mini-GBIC Ports: Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches (see Section 3.1.3 on page 47 for instructions).

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Gigabit Ethernet Ports

The Switch has 10/100/1000 Mbps auto-negotiating, auto-crossover Gigabit Ethernet ports. In 10/100/1000 Mbps Gigabit Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the Switch are:

- Speed: Auto
- Duplex: Auto

- Flow control: on

3.1.3 SFP Slots

The Switch comes with SFP (Small Form-factor Pluggable) slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the SFP transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

SFP transceivers can be standalone interfaces or part of a dual personality interface. Each dual personality interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber slot for mini-GBIC transceivers, with one port active at a time. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)



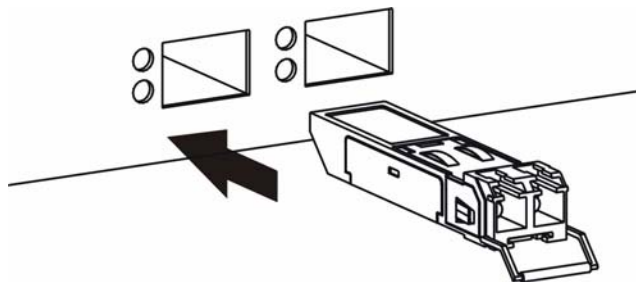
To avoid possible eye injury, do NOT look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

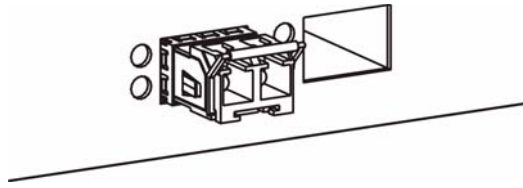
Use the following steps to install a mini-GBIC transceiver (SFP module).

- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

Figure 10 Transceiver Installation Example



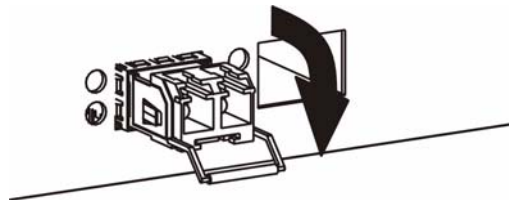
- 2 Press the transceiver firmly until it clicks into place.
- 3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 11 Installed Transceiver

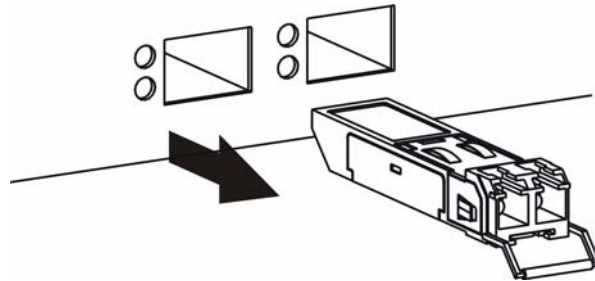
3.1.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

- 1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example

- 2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example

3.2 Rear Panel

The following figures show the rear panels of the AC and DC power input model switches. The rear panel contains a connector for backup power supply (BPS) and the power receptacle. For the DC power input model, it also contains the power switch.

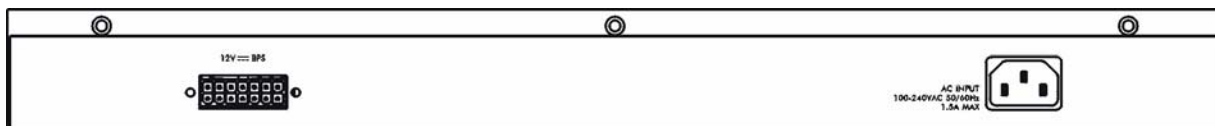
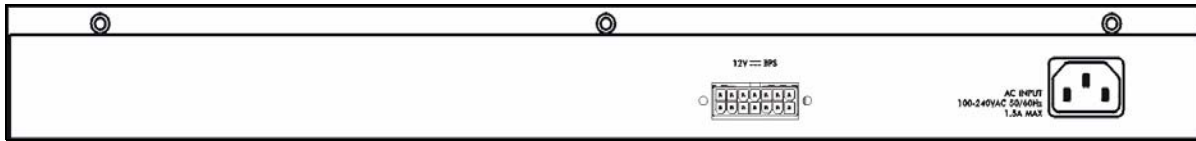
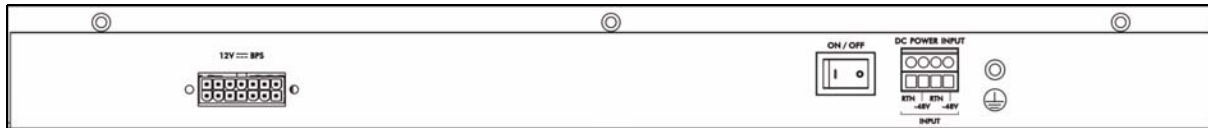
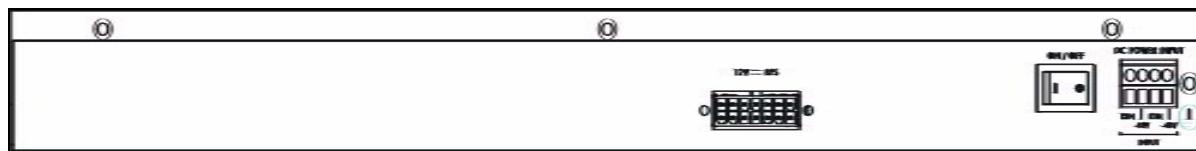
Figure 14 Rear Panel: GS-4012F

Figure 15 Rear Panel: GS-4024**Figure 16** Rear Panel: GS-4012F (DC Model)**Figure 17** Rear Panel: GS-4024 (DC Model)

3.3 Power Connections Overview

Use the following procedures to connect the Switch to a power source after you have installed it. Make sure that no objects obstruct the airflow of the fans.



Check the power supply requirements in [Appendix A on page 425](#), and make sure you are using an appropriate power source.

Keep the power supply switch and the Switch's power switch in the OFF position until you come to the procedure for turning on the power.

3.3.1 AC Power Connection



This is only for the AC models of the Switch.

To connect the power to the Switch, connect the female end of the power cord to the power socket of your Switch. Connect the other end of the power cord to a power outlet.

3.3.2 DC Power Connection



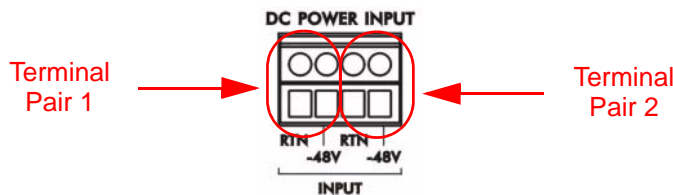
This is only for the DC model of the Switch.

The DC-powered unit uses a single terminal block with four terminals which allows you to connect two power supplies. If one power supply fails the system can operate on the remaining power supply. Use two wires to connect a single terminal pair, one wire for the positive terminal and one wire for the negative terminal.



The current rating of the power wires must be greater than 20 Amps. The power supply to which the Switch connects must have a built-in circuit breaker or switch to toggle the power.

Figure 18 Terminal Block Pairs



When installing the Switch power wire, push the wire firmly into the terminal as deep as possible and make sure that no exposed (bare) wire can be seen or touched.

Exposed power wire is dangerous. Use extreme care when connecting a DC power source to the device.

To connect a power supply:

- 1 Use a screwdriver to loosen the screws on a terminal pair.
- 2 Connect one end of a power wire to the Switch's **RTN** (return) terminal and tighten the terminal screw.
- 3 Connect the other end of the power wire to the positive terminal on the power supply.
- 4 Connect one end of a power wire to the Switch's **-48V** (input) terminal and tighten the terminal screw.
- 5 Connect the other end of the power wire to the negative terminal on the power supply.
- 6 Insert the terminal block plug in the Switch's terminal block header.

3.3.3 External Backup Power Supply Connector

The backup power supply constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the Switch in the event of a power failure. Once the Switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

3.3.4 Powering on the Switch

- 1 Turn on the power supply first.
- 2 Turn the Switch power on second.

3.4 LEDs

The following table describes the LEDs.

Table 2 LEDs

LED	COLOR	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
MGMT Port			
10	Green	On	The link to a 10 Mbps Ethernet network is up.
		Blinking	The port is sending or receiving data at 10 Mbps.
		Off	The link to a 10 Mbps Ethernet network is down.
100	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The port is sending or receiving data at 100 Mbps.
		Off	The link to a 100 Mbps Ethernet network is down.
GS-4024 Model			
Gigabit Ethernet Ports			
LNK/ACT	Green	On	The port has a successful 10/1000 Mbps connection.
	Amber	On	The port has a successful 100 Mbps connection.
		Blinking	The port is sending or receiving data.
		Off	The port is disconnected or the link failed.
FDX	Amber	On	The port is in full duplex mode.
		Off	The port is in half duplex mode or there is no connection.

Table 2 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Mini-GBIC (SFP) Slots			
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data or there is no connection.
GS-4012F Model			
Mini-GBIC (SFP) Slots (Standalone and Part of Dual Personality Interface)			
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data or there is no connection.
Gigabit Ethernet Ports (Part of Dual Personality Interface)			
1000	Green	Blinking	The port is sending/receiving data.
		On	The link to a 10/1000 Mbps Ethernet network is up.
		Off	The link to a 10/1000 Mbps Ethernet network is down.
100	Amber	Blinking	The port is sending/receiving data.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.

PART II

Basic Configuration

The Web Configurator (55)
Initial Setup Example (65)
System Status and Port Statistics (71)
Basic Setting (77)

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

- 1 Start your web browser.
- 2 Type “http://” and the IP address of the Switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].
- 3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

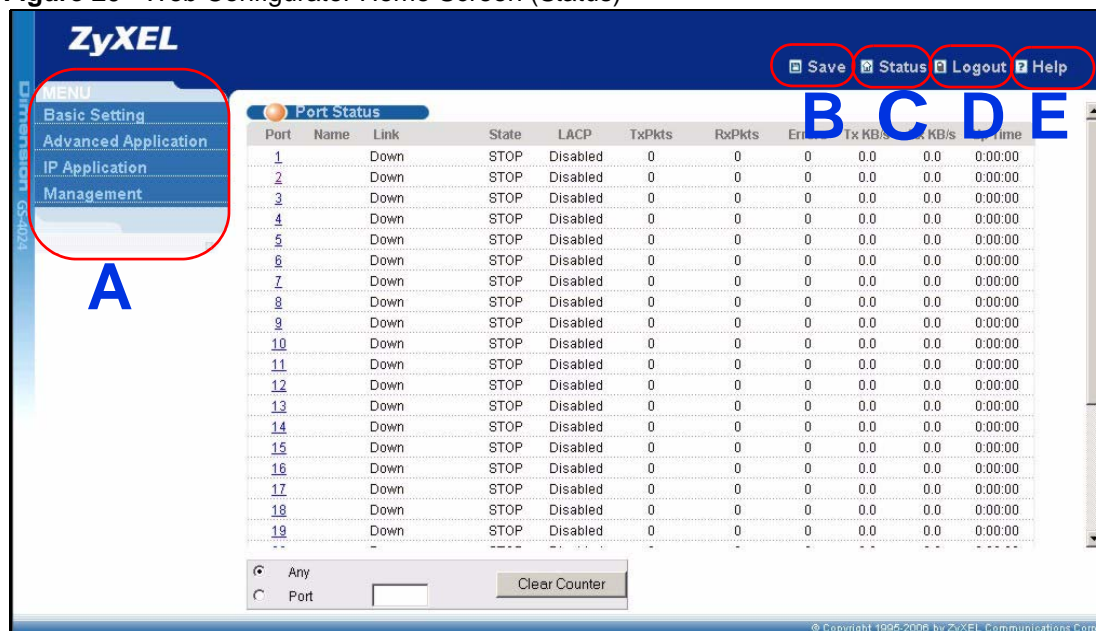
Figure 19 Web Configurator: Login

- 4 Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

Figure 20 Web Configurator Home Screen (Status)

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.





B, C, D, E - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

- C** - Click this link to go to the status page of the Switch.
- D** - Click this link to logout of the web configurator.
- E** - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 3 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table lists the various web configurator screens within the sub-links.

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
System Info General Setup Switch Setup IP Setup Port Setup	VLAN VLAN Port Setting Subnet Based VLAN Static VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Configuration RSTP MRSTP MSTP Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Link Aggregation Setting Link Aggregation Control Protocol Port Authentication 802.1x MAC Authentication Port Security Classifier Policy Rule Queuing Method VLAN Stacking Multicast Multicast Setting IGMP Snooping VLAN IGMP Filtering Profile MVR Group Configuration Authentication and Accounting RADIUS Server Setup TACACS+ Server Setup Auth and Acct Setup IP Source Guard IP Source Guard Static Binding DHCP Snooping ARP Inspection Status Loop Guard	Static Routing RIP OSPF Status OSPF Configuration OSPF Interface OSPF Virtual Link IGMP DVMRP IP Multicast DiffServ 2-Rate 3 Color Marker DSCP Setting DHCP Status DHCP Relay VLAN Setting VRRP VRRP Configuration	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Save Configuration Reboot System Access Control SNMP Logins Service Access Control Remote Management Diagnostic Syslog Syslog Server Setup Cluster Management Clustering Management Configuration MAC Table IP Table ARP Table Routing Table Configure Clone

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to a screen where you can configure VLAN stacking.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Auth and Acct	This link takes you to a screen where you can configure authentication and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
IP Multicast	This link takes you to a screen where you can configure the Switch to remove VLAN tags from IP multicast packets on an out-going port.
DiffServ	This link takes you to screens where you can enable DiffServ, configure 2-Rate 3 Color Marker and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to screens where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
IP Table	This link takes you to a screen where you can view the IP addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management**, **Access Control** and then **Logins** to display the next screen.

Figure 21 Change Administrator Login Password

Logins [Access Control](#)

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.



Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

- 1 Delete the management VLAN (default is VLAN 1).
- 2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
- 3 Filter all traffic to the CPU port.
- 4 Disable all ports.
- 5 Misconfigure the text configuration file.

- 6 Forget the password and/or IP address.
- 7 Prevent all services from accessing the Switch.
- 8 Change a service port number but forget it.



Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software. See [Section 3.1.1 on page 46](#) for details.
- 2 Disconnect and reconnect the Switch’s power to begin a session. When you reconnect the Switch’s power, you will see the initial screen.
- 3 When you see the message “Press any key to enter Debug Mode within 3 seconds ...” press any key to enter debug mode.
- 4 Type `atlc` after the “Enter Debug Mode” message.
- 5 Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
- 6 After a configuration file upload, type `atgo` to restart the Switch.

Figure 22 Resetting the Switch: Via the Console Port

```

Bootbase Version: V3.1 | 03/08/2007 18:36:17
RAM:Size = 64 Mbytes
DRAM POST: Testing: 65536K OK
DRAM Test SUCCESS !
FLASH: Intel 64M
ZyNOS Version: V3.80(TS.0)b4 | 03/31/2007 20:43:39
Press any key to enter debug mode within 3 seconds.....
Enter Debug Mode
GS-4024> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
GS-4024> atgo

```

The Switch is now reinitialized with a default configuration file including the default password of “1234”.

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 23 Web Configurator: Logout Screen

4.8 Help

The web configurator’s online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

Initial Setup Example

This chapter shows how to set up the Switch for an example network.

5.1 Overview

The following lists the configuration steps for the example network:

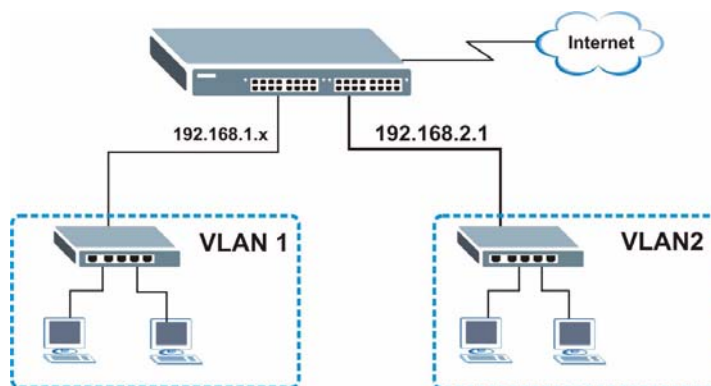
- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID
- Enable RIP

5.1.1 Configuring an IP Interface

On a layer-3 Switch, an IP interface (also known as an IP routing domain) is not bound to a physical port. The default IP address of the Switch is 192.168.1.1 with a subnet mask of 255.255.255.0.

In the example network, since the **RD** network is already in the same IP interface as the Switch, you don't need to create an IP interface for it. However, if you want to have the **Sales** network on a different routing domain, you need to create a new IP interface. This allows the Switch to route traffic between the **RD** and **Sales** networks.

Figure 24 Initial Setup Network Example: IP Interface



- 1 Connect your computer to the **MGMT** port that is used only for management. Make sure your computer is in the same subnet as the **MGMT** port.

- 2 Open your web browser and enter 192.168.0.1 (the default **MGMT** port IP address) in the address bar to access the web configurator. See [Section 4.2 on page 55](#) for more information.
- 3 Click **Basic Setting** and **IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.
For the **Sales** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 5 In the **VID** field, enter the ID of the VLAN group to which you want this IP interface to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 6 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.2 Configuring DHCP Server Settings

You can set the Switch to assign network information (such as the IP address, DNS server, etc.) to DHCP clients on the network.

For the example network, configure two DHCP client pools on the Switch for the DHCP clients in the **RD** and **Sales** networks.

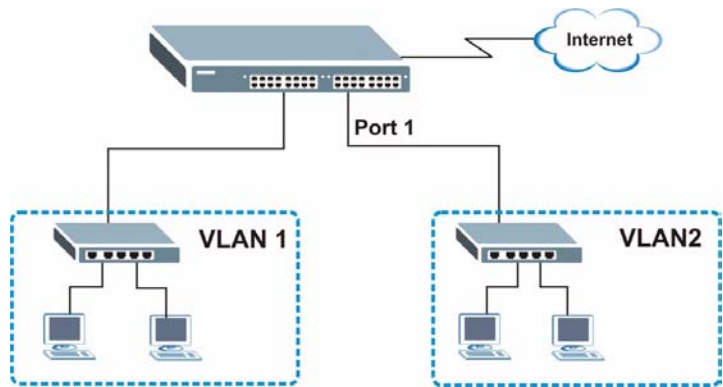
- 1 In the web configurator, click **IP Application** and **DHCP** in the navigation panel and click the **VLAN** link.
- 2 In the **VLAN Setting** screen, specify the ID of the VLAN to which the DHCP clients belong, the starting IP address pool, subnet mask, default gateway address and the DNS server address(es).
- 3 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.3 Creating a VLAN

VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

Figure 25 Initial Setup Network Example: VLAN



- 1 Click **Advanced Application** and **VLAN** in the navigation panel and click the **Static VLAN** link.

The screenshot shows the 'Static VLAN' configuration screen. At the top, there are tabs for 'VLAN Status', 'VLAN Port Setting', and 'Static VLAN' (which is selected). Below the tabs, a table displays the current VLAN configuration:

Index	VID	Elapsed Time	Status
1	1	1:00:31	Static

At the bottom, there are navigation buttons: 'Change Pages', 'Previous', and 'Next'.

- 2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.

The screenshot shows the 'Static VLAN' configuration screen. At the top, there are tabs for 'Static VLAN' and 'VLAN Status' (which is selected). Below the tabs, the configuration fields are as follows:

- ACTIVE**: ☒
- Name**: Example
- VLAN Group ID**: 2

Below these fields is a table for port configuration:

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging



The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

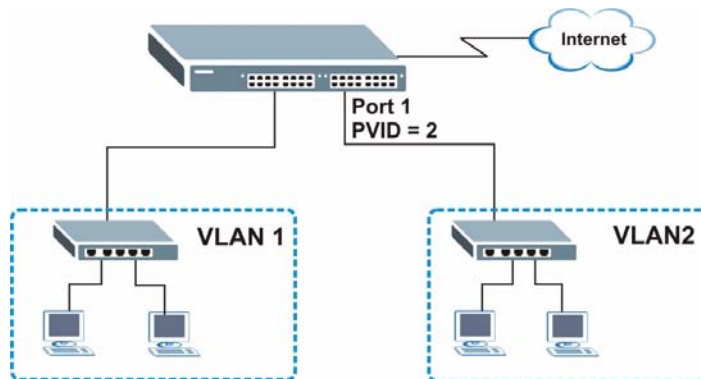
- 3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.
- 5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.4 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 26 Initial Setup Network Example: Port VID



- 1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
- 2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

VLAN Port Setting						VLAN Status
GVRP <input type="checkbox"/>						
Port isolation <input type="checkbox"/>						
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	
1	<input type="checkbox"/>	2	<input type="checkbox"/>	All	<input type="checkbox"/>	
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>	

5.1.5 Enabling RIP

To exchange routing information with other routing devices across different routing domains, enable RIP (Routing Information Protocol) in the **RIP** screen.

1 Click **IP Application > RIP** in the navigation panel.

2 Select **Both** in the **Direction** field to set the Switch to broadcast and receive routing information.

3 In the **Version** field, select **RIP-1** for the RIP packet format that is universally supported.

4 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Index	Network	Direction	Version
1	172.23.19.95/24	Both	RIP-1
2	192.168.1.1/24	Both	RIP-1

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

6.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

6.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 27 Status

Port Status										
Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

☒ Any
 ☐ Port

The following table describes the labels in this screen.

Table 6 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen (refer to Figure 28 on page 73).
Name	This is the name you assigned to this port in the Basic Setting, Port Setup screen.

Table 6 Status (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half). It also shows the cable type (Copper or Fiber) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1 on page 109 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Enter a port number and then click Clear Counter to erase the recorded statistical information for that port, or select Any to clear statistics for all ports.

6.2.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 28 Status > Port Details

Port Details		Port Status
Port Info	Port NO.	1
	Name	
	Link	Down
	Status	STOP
	LACP	Disabled
	TxPkts	0
	RxPkts	0
	Errors	0
	Tx KB/s	0.0
	Rx KB/s	0.0
	Up Time	0:00:00
TX Packet	TX Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
RX Packet	RX Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	0
	65 to 127	0
	128 to 255	0
	256 to 511	0
	512 to 1023	0
	1024 to 1518	0
	Giant	0

The following table describes the labels in this screen.

Table 7 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half duplex). It also shows the cable type (Copper or Fiber).
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1 on page 109 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX Packet	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packet	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

Basic Setting

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

7.1 Overview

The **System Info** screen displays general Switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general Switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your Switch. The real time is then displayed in the Switch logs. The **Switch Setup** screen allows you to set up and configure global Switch features. The **IP Setup** screen allows you to configure a Switch IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** and **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen.

Figure 29 System Info

System Info

System Name

ZyNOS FW Version

Ethernet Address

GS-4012F

V3.80(TS.0)b4 | 03/31/2007

00:19:cb:00:00:02

Hardware Monitor

Temperature Unit

C

Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	35.0	36.0	26.0	65.0	Normal
CPU	34.0	34.5	25.0	65.0	Normal
PHY	40.0	40.5	28.5	65.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	6450	6510	6194	3250	Normal
FAN2	6392	6450	6167	3250	Normal
FAN3	6540	6571	6334	3250	Normal
Voltage (V)	Current	MAX	MIN	Threshold	Status
VCOREA	2.576	2.576	2.576	+/-8%	Normal
VINRO	1.232	1.232	1.232	+/-11%	Normal
3.3VIN	3.344	3.344	3.344	+/-7%	Normal
AVCC	4.972	4.972	4.972	+/-7%	Normal
+12VIN	12.342	12.342	12.281	+/-11%	Normal
-12VIN	1.248	1.248	1.248	+/-8%	Normal
5VSB	1.328	1.328	1.328	+/-10%	Normal
-5VIN	1.248	1.248	1.248	+/-8%	Normal
VBAT	--	--	--	--	Absent

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	MAC , CPU and PHY refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.

Table 8 System Info (continued)

LABEL	DESCRIPTION
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.

7.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** > **General Setup** in the navigation panel to display the screen as shown.

Figure 30 Basic Setting > General Setup

General Setup

System Name

Location

Contact Person's Name

Use Time Server when Bootup None

Time Server IP Address

Current Time 00 : 56 : 23 UTC

New Time (hh:mm:ss) 00 : 56 : 23

Current Date 1970 - 01 - 01

New Date (yyy-mm-dd) 1970 - 01 - 01

Time Zone UTC

Daylight Saving Time ☐

Start Date First Sunday of January at 0:00

End Date First Sunday of January at 0:00

It will take 60 seconds if time server is unreachable.

The following table describes the labels in this screen.

Table 9 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	<p>Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format.</p> <p>When you select the Daytime (RFC 867) format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0.</p>
Time Server IP Address	Enter the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

Table 9 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time . The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00 . Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

7.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.



VLAN is unidirectional; it only governs outgoing traffic.

See [Chapter 8 on page 91](#) for information on port-based and 802.1Q tagged VLANs.

7.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

Figure 31 Basic Setting > Switch Setup

The following table describes the labels in this screen.

Table 10 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. See Chapter 8 on page 91 for more information.
Bridge Control Protocol Transparency	Select Active to allow the Switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the Port Setup screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.

Table 10 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Priority Queue Assignment	IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

7.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

7.6.1 IP Interfaces

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

On the Switch, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

Figure 32 Basic Setting > IP Setup

IP Setup

Default Gateway: 0.0.0.0

Domain Name Server: 0.0.0.0

Default Management: ☒ In-band ☐ Out-of-band

Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

IP Interface

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

VID:

Add Cancel

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.12	255.255.255.0	1	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 11 Basic Setting > IP Setup

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (In-Band or Out-of-band) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select Out-of-band to have the Switch send the packets to the management port labelled MGMT . This means that device(s) connected to the other port(s) do not receive these packets. Select In-Band to have the Switch send the packets to all ports except the management port (labelled MGMT) to which connected device(s) do not receive these packets.
Management IP Address Use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.0.254

Table 11 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
IP Interface Use these fields to create or edit IP routing domains on the Switch.	
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation. For example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Delete	Click Delete to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out from the Switch.
Cancel	Click Cancel to clear the Delete check boxes.

7.7 Port Setup

Use this screen to configure Switch port settings. Click **Basic Setting** and then **Port Setup** in the navigation panel to display the configuration screen.

Figure 33 Basic Setting > Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
*	<input type="checkbox"/>		-	Auto	<input type="checkbox"/>	0	Peer
1	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
2	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
3	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
4	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
5	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
6	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
7	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
8	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer

Apply Cancel

The following table describes the labels in this screen.

Table 12 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	<p>Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	<p>Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters.</p> <p>Note: Due to space limitation, the port name may be truncated in some web configurator screens.</p>
Type	This field displays 10/100/1000M for Gigabit connections.
Speed/Duplex	<p>Select the speed and the duplex mode of the Ethernet connection on this port. Choices are Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex, 100M/Full Duplex and 1000M/Full Duplex.</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>

Table 12 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.</p>
802.1p Priority	<p>This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 10 on page 82 for more information.</p>
BPDU Control	<p>Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first.</p> <p>Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port.</p> <p>Select Tunnel to forward BPDUs received on this port.</p> <p>Select Discard to drop any BPDU received on this port.</p> <p>Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Apply	<p>Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

PART III

Advanced

VLAN (91)
Static MAC Forward Setup (105)
Filtering (107)
Spanning Tree Protocol (109)
Bandwidth Control (127)
Broadcast Storm Control (129)
Mirroring (131)
Link Aggregation (133)
Port Authentication (141)
Port Security (147)
Classifier (151)
Policy Rule (157)
Queuing Method (163)
VLAN Stacking (165)
Multicast (171)
Authentication & Accounting (185)
IP Source Guard (199)
Loop Guard (219)

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

8.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

8.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

8.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

8.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

8.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

8.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 13 IEEE 802.1Q VLAN Terminology

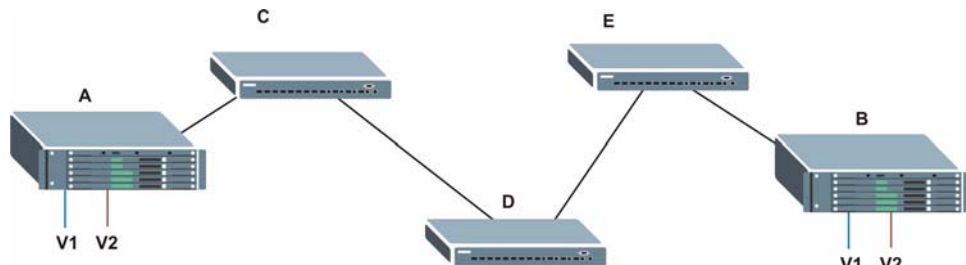
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member

8.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Figure 34 Port VLAN Trunking



8.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting > Switch Setup** screen.

Figure 35 Switch Setup: Select VLAN Type



8.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

8.5.1 Static VLAN Status

See [Section 8.1 on page 91](#) for more information on Static VLAN. Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 36 Advanced Application > VLAN: VLAN Status

Index	VID	Elapsed Time	Status
1	1	3:49:44	Static

The following table describes the labels in this screen.

Table 14 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the Switch.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; dynamic - using GVRP, static - added as a permanent entry or other - added in another way such as via Multicast VLAN Registration (MVR).
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Static VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See [Section 8.1 on page 91](#) for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 37 Advanced Application > VLAN > VLAN Detail

VID	Port Number												Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24		
1	U	U	U	U	U	U	U	U	U	U	U	U	2:12:57	Static
	U	U	U	U	U	U	U	U	U	U	U	U		
	U	U	U	U	U	U	U	U	U	U	U	U		

The following table describes the labels in this screen.

Table 15 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the VLAN Status screen.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN are marked as “—”.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; dynamic - using GVRP, static - added as a permanent entry or other - added in another way such as via Multicast VLAN Registration (MVR).

8.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See [Section 8.1 on page 91](#) for more information on static VLAN. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 38 Advanced Application > VLAN > Static VLAN

Static VLAN VLAN Status

ACTIVE ☐

Name

VLAN Group ID

Port	Control	Tagging
*	Normal	<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

Add Cancel Clear

VID	Active	Name	Delete
1	Yes	1	<input type="checkbox"/>

Delete Cancel

The following table describes the related labels in this screen.

Table 16 Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to change the fields back to their last saved values.
Clear	Click Clear to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

8.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See [Section 8.1 on page 91](#) for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 39 Advanced Application > VLAN > VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 17 Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port Isolation	Port Isolation allows each port to communicate only with the CPU management port and the dual personality GbE interfaces but not communicate with each other. This option is the most limiting but also the most secure.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.

Table 17 Advanced Application > VLAN > VLAN Port Setting (continued)

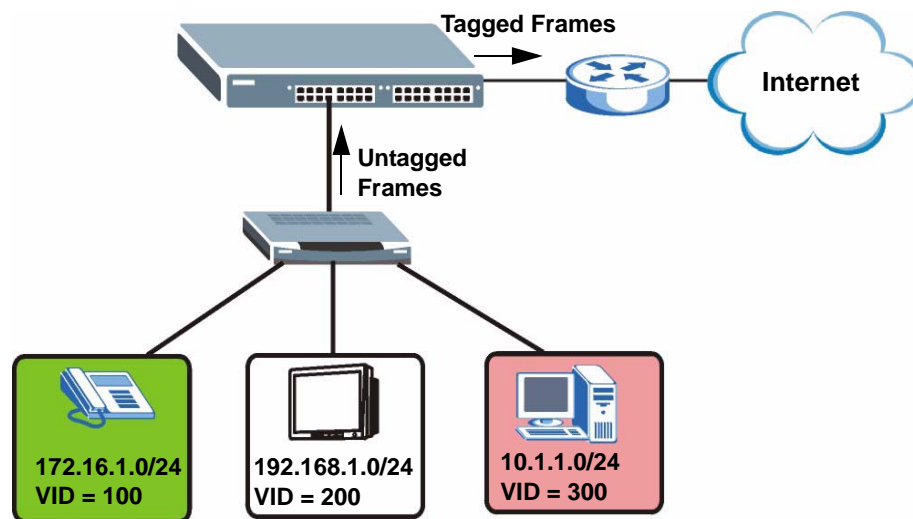
LABEL	DESCRIPTION
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

8.6 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

Figure 40 Subnet Based VLAN Application Example

8.7 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.



Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

Figure 41 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN

The screenshot shows the 'Subnet Based VLAN' configuration interface. At the top, there's a header with 'Subnet Based VLAN' and 'Vlan Port Setting'. Below this, there are two checkboxes: 'Active' and 'DHCP-Vlan Override', each with an 'Apply' button next to it. Underneath, there's a table with columns: Index, Active, Name, IP, Mask-Bits, VID, Priority, and Delete. Below the table, there are 'Add' and 'Cancel' buttons. At the bottom, there are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 18 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Check this box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Check this box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alpha numeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.

Table 18 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the Advanced Applications, VLAN screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click Cancel to begin configuring this screen afresh.

8.8 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.



When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.



In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

8.8.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN** from the navigation panel to display the next screen.

Figure 42 Port Based VLAN Setup (All Connected)

The screenshot shows the 'Port Based VLAN Setup' window. At the top, there's a 'Setting Wizard' section with a dropdown menu set to 'All connected' and an 'Apply' button. Below this is a large grid for configuring VLANs. The grid has two main sections: 'Incoming' and 'Outgoing'. Each section has 24 rows and 24 columns. The rows are numbered 1 to 24, and the columns are numbered 1 to 24. The 'CPU' port is listed at the bottom of each section. All cells in the grid contain a checked checkbox, indicating that all ports are connected. At the bottom of the grid, there are 'Apply' and 'Cancel' buttons.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		
Incoming	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1	
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3	
	4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	4	
	5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	5	
	6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	6
	7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	7
	8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	8
	9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	9
	10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
	11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	11
	12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
	13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	13
	14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Outgoing	15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	15	
	16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	16	
	17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	
	18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18	
	19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	19	
	20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	20
	21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21
	22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	22
	23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	23
	24	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	24
CPU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	CPU	

Figure 43 Port Based VLAN Setup (Port Isolation)

The following table describes the labels in this screen.

Table 19 Port Based VLAN Setup

label	Description
Setting Wizard	<p>Choose All connected or Port isolation.</p> <p>All connected means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure.</p> <p>Port isolation means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure.</p> <p>After you make your selection, click Apply (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click Apply at the bottom of the screen.</p>
Incoming	<p>These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). CPU refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.</p>

Table 19 Port Based VLAN Setup (continued)

label	Description
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

9.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

9.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See [Chapter 17 on page 147](#) for more information on port security.

Click **Advanced Applications > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 44 Advanced Application > Static MAC Forwarding

Index	Active	Name	MAC Address	VID	Port	Delete

The following table describes the labels in this screen.

Table 20 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click Add to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

Filtering

This chapter discusses MAC address port filtering.

10.1 Configure a Filtering Rule

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

Click **Advanced Application > Filtering** in the navigation panel to display the screen as shown next.

Figure 45 Advanced Application > Filtering

The screenshot shows the 'Filtering' configuration interface. It includes a title bar, a form with fields for 'Active', 'Name', 'Action', 'MAC', and 'VID', and a table at the bottom for listing rules. The 'Active' field is a checkbox. The 'Name' field is a text input. The 'Action' field has two checkboxes: 'Discard source' and 'Discard destination'. The 'MAC' field is a text input with colons. The 'VID' field is a text input. Below the form are 'Add', 'Cancel', and 'Clear' buttons. The table at the bottom has columns: Index, Active, Name, MAC Address, VID, Action, and Delete. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the related labels in this screen.

Table 21 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.

Table 21 Advanced Application > Filtering (continued)

LABEL	DESCRIPTION
Action	<p>Select Discard source to drop frame from the source MAC address (specified in the MAC field). The Switch can still send frames to the MAC address.</p> <p>Select Discard destination to drop frames to the destination MAC address (specified in the MAC address). The Switch can still receive frames originating from the MAC address.</p> <p>Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.</p>
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es) in the Delete column.

Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

11.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.



In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 22 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 23 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.1.4 Multiple RSTP

MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

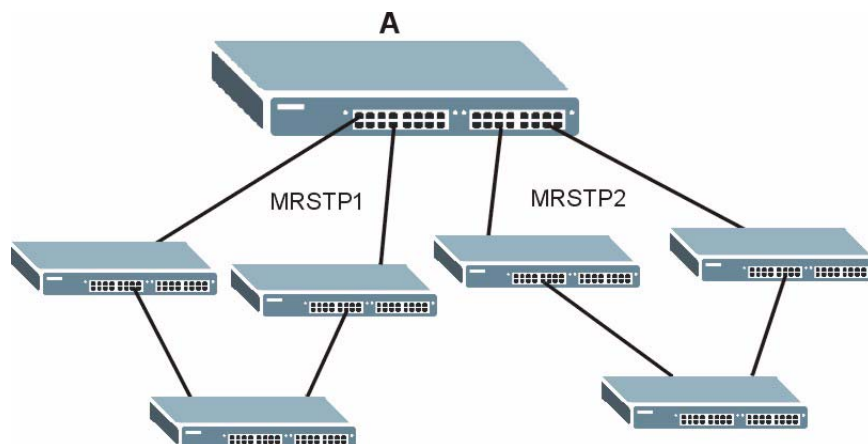
In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.



Each port can belong to one STP tree only.

Figure 46 MRSTP Network Example



11.1.5 Multiple STP

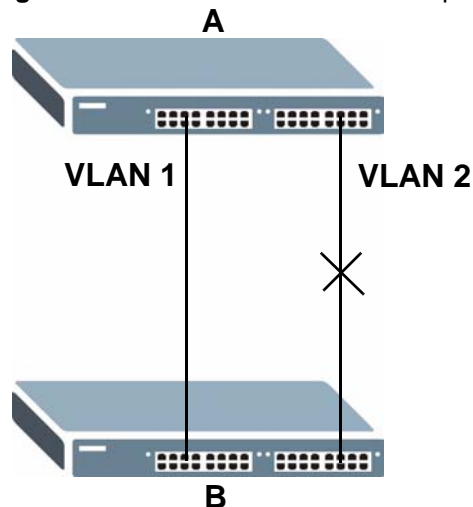
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

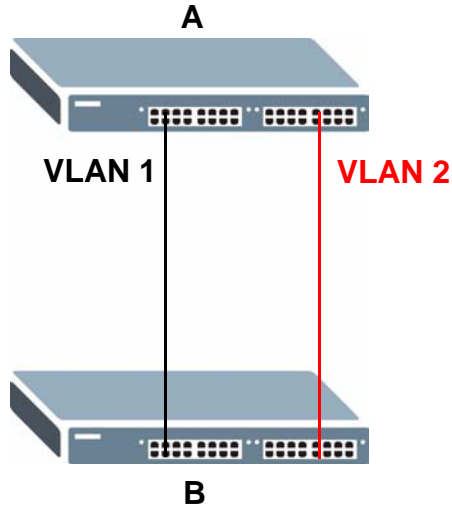
11.1.5.1 MSTP Network Example

The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 47 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 48 MSTP Network Example

11.1.5.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

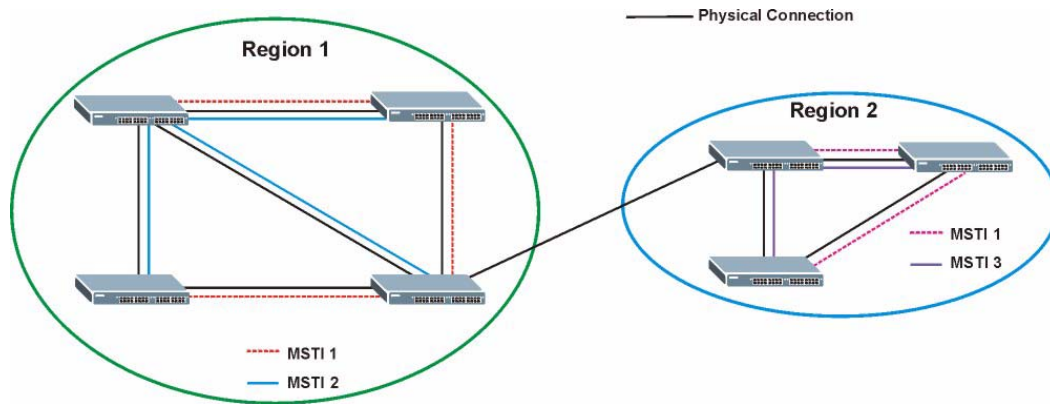
Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

11.1.5.3 MST Instance

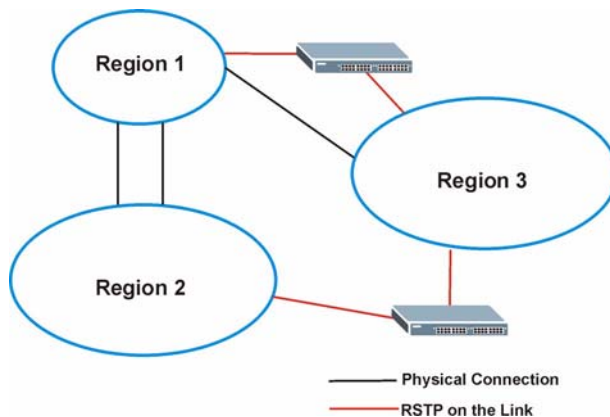
An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

Figure 49 MSTIs in Different Regions

11.1.5.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

Figure 50 MSTP and Legacy RSTP Network Example

11.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application > Spanning Tree Protocol** to see the screen as shown.

Figure 51 Advanced Application > Spanning Tree Protocol

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times	0	
Time Since Last Change	0:00:00	

This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

11.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application > Spanning Tree Protocol**.

Figure 52 Advanced Application > Spanning Tree Protocol > Configuration

The following table describes the labels in this screen.

Table 24 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select Rapid Spanning Tree , Multiple Rapid Spanning Tree or Multiple Spanning Tree . See Section 11.1 on page 109 for background information on STP.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 11.1 on page 109](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

Figure 53 Advanced Application > Spanning Tree Protocol > RSTP

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	128	4
2	<input checked="" type="checkbox"/>	128	4
3	<input checked="" type="checkbox"/>	128	4
4	<input checked="" type="checkbox"/>	128	4
5	<input type="checkbox"/>	128	4
6	<input type="checkbox"/>	128	4
7	<input type="checkbox"/>	128	4
8	<input type="checkbox"/>	128	4

The following table describes the labels in this screen.

Table 25 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 54 on page 118).
Active	<p>Select this check box to activate RSTP. Clear this checkbox to disable RSTP.</p> <p>Note: You must also activate Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable RSTP on the Switch.</p>
Bridge Priority	<p>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>

Table 25 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	<p>This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.</p> <p>As a general rule:</p> <p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this check box to activate RSTP on this port.
Priority	<p>Configure the priority for each port here.</p> <p>Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.</p>
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 22 on page 110 for more information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 109](#) for more information on RSTP.



This screen is only available after you activate RSTP on the Switch.

Figure 54 Advanced Application > Spanning Tree Protocol > Status: RSTP

Spanning Tree Protocol Status			Configuration	RSTP	MRSTP	MSTP
Spanning Tree Protocol: RSTP						
Bridge	Root		Our Bridge			
Bridge ID	0000-000000000000		0000-000000000000			
Hello Time (second)	0		0			
Max Age (second)	0		0			
Forwarding Delay (second)	0		0			
Cost to Bridge	0					
Port ID	0x0000					
Topology Changed Times	0					
Time Since Last Change	0:00:00					

The following table describes the labels in this screen.

Table 26 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click RSTP to edit RSTP settings on the Switch.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 11.1 on page 109](#) for more information on MRSTP.

Figure 55 Advanced Application > Spanning Tree Protocol > MRSTP

Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
2	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
3	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
4	<input type="checkbox"/>	32768	2 seconds	20 seconds	15

Port	Active	Priority	Path Cost	Tree
*	<input type="checkbox"/>			1
1	<input type="checkbox"/>	128	4	1
2	<input type="checkbox"/>	128	4	1
3	<input type="checkbox"/>	128	4	1
4	<input type="checkbox"/>	128	4	1
5	<input type="checkbox"/>	128	4	1
6	<input type="checkbox"/>	128	4	1
7	<input type="checkbox"/>	128	4	1
8	<input type="checkbox"/>	128	4	1

Apply Cancel

The following table describes the labels in this screen.

Table 27 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click Status to display the MRSTP Status screen (see Figure 54 on page 118).
Tree	This is a read only index number of the STP trees.
Active	<p>Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree.</p> <p>Note: You must also activate Multiple Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MRSTP on the Switch.</p>
Bridge Priority	<p>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Table 27 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	<p>This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.</p> <p>As a general rule:</p> <p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this check box to activate STP on this port.
Priority	<p>Configure the priority for each port here.</p> <p>Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.</p>
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 22 on page 110 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 109](#) for more information on MRSTP.



This screen is only available after you activate MRSTP on the Switch.

Figure 56 Advanced Application > Spanning Tree Protocol > Status: MRSTP

Spanning Tree Protocol Status			Configuration	RSTP	MRSTP	MSTP
Spanning Tree Protocol: MRSTP						
Tree	1					
Bridge	Root		Our Bridge			
Bridge ID	8000-001349000002		8000-001349000002			
Hello Time (second)	2		2			
Max Age (second)	20		20			
Forwarding Delay (second)	15		15			
Cost to Bridge	0					
Port ID	0x0000					
Topology Changed Times	0					
Time Since Last Change	0:00:00					

The following table describes the labels in this screen.

Table 28 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click MRSTP to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 11.1.5 on page 112](#) for more information on MSTP.

Figure 57 Advanced Application > Spanning Tree Protocol > MSTP

Multiple Spanning Tree Protocol

Status

Bridge:

Active

☐

Hello Time

2

seconds

MAX Age

20

seconds

Forwarding Delay

15

seconds

Maximum hops

128

Configuration Name

001349000002

Revision Number

0

Apply

Cancel

Instance:

Instance

0

Bridge Priority

0

VLAN Range

Start

End

Add

Remove

Clear

Enabled VLAN(s)

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>		
1	<input type="checkbox"/>	128	19
2	<input type="checkbox"/>	128	19
3	<input type="checkbox"/>	128	19
4	<input type="checkbox"/>	128	19
5	<input type="checkbox"/>	128	19
6	<input type="checkbox"/>	128	19
7	<input type="checkbox"/>	128	19
8	<input type="checkbox"/>	128	19

Add

Cancel

The following table describes the labels in this screen.

Table 29 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click Status to display the MSTP Status screen (see Figure 58 on page 125).
Active	<p>Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch.</p> <p>Note: You must also activate Multiple Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MSTP on the Switch.</p>
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	<p>This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule:</p> <p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.
Bridge Priority	<p>Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance.</p> <p>Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).</p>

Table 29 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the Start field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the End field. Next click: <ul style="list-style-type: none"> • Add - to add this range of VLAN(s) to be mapped to the MST instance. • Remove - to remove this range of VLAN(s) from being mapped to the MST instance. • Clear - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 22 on page 110 for more information.
Add	Click Add to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

11.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1.5 on page 112](#) for more information on MSTP.



This screen is only available after you activate MSTP on the Switch.

Figure 58 Advanced Application > Spanning Tree Protocol > Status: MSTP

Spanning Tree Protocol Status [Configuration](#) [RSTP](#) [MRSTP](#) [MSTP](#)

Spanning Tree Protocol: MSTP

CST

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	8000-000000000000
Hello Time (second)	0	2
Max Age (second)	0	20
Forwarding Delay (second)	0	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	001349000002	
Revision Number	0	
Configuration Digest	A317523DB32DA2D62	
Topology Changed Times	0	
Time Since Last Change	0	

Instance:

Instance	VLAN
0	1-4093

MSTI 1

Bridge	Regional Root	Our Bridge
Bridge ID	0000-000000000000	8001-000000000000
Internal Cost	0	0
Port ID	0x0000	0x0000

The following table describes the labels in this screen.

Table 30 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click MSTP to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.

Table 30 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	Root refers to the base of the MST instance. Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.



The CIR should be less than the PIR. The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

12.2 Bandwidth Control Setup

Click **Advanced Application > Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 59 Advanced Application > Bandwidth Control

Port	Ingress Rate				Egress Rate	
	Active	Commit Rate	Active	Peak Rate	Active	Egress Rate
*	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
1	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
2	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
3	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
4	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
5	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
6	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
7	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps
8	<input type="checkbox"/>	1 Kbps	<input type="checkbox"/>	1000 Kbps	<input type="checkbox"/>	1000 Kbps

The following table describes the related labels in this screen.

Table 31 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

13.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

Click **Advanced Application > Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 60 Advanced Application > Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>	<input type="checkbox"/> <input type="text"/>
1	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
2	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
3	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
4	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
5	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
6	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
7	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>
8	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>	<input type="checkbox"/> <input type="text" value="0"/>

The following table describes the labels in this screen.

Table 32 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

Mirroring

This chapter discusses port mirroring setup screens.

14.1 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Advanced Application > Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 61 Advanced Application > Mirroring

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input type="checkbox"/>	Ingress ▼
2	<input type="checkbox"/>	Ingress ▼
3	<input type="checkbox"/>	Ingress ▼
4	<input type="checkbox"/>	Ingress ▼
5	<input type="checkbox"/>	Ingress ▼
6	<input type="checkbox"/>	Ingress ▼
7	<input type="checkbox"/>	Ingress ▼
8	<input type="checkbox"/>	Ingress ▼

Apply Cancel

The following table describes the labels in this screen.

Table 33 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

15.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The Switch supports both static and dynamic link aggregation.



In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See [Section 15.6 on page 138](#) for a static port trunking example.

15.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 34 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

Table 35 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

15.3 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 15.1 on page 133](#) for more information.

Figure 62 Advanced Application > Link Aggregation Status

Index	Enabled Ports	Synchronized Ports	Aggregator ID	Status
1	-	-	-	-
2	-	-	-	-
3	-	-	-	-
4	-	-	-	-
5	-	-	-	-
6	-	-	-	-

The following table describes the labels in this screen.

Table 36 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the Link Aggregation screen to be in the trunk group.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Table 36 Advanced Application > Link Aggregation Status (continued)

LABEL	DESCRIPTION
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 134 for more information on this field.
Status	This field displays how these ports were added to the trunk group. It displays: <ul style="list-style-type: none"> • Static - if the ports are configured as static members of a trunk group. • LACP - if the ports are configured to join a trunk group via LACP.

15.4 Link Aggregation Setting

Click **Advanced Application > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 15.1 on page 133](#) for more information on link aggregation.

Figure 63 Advanced Application > Link Aggregation > Link Aggregation Setting

Link Aggregation Setting Status LACP

Group ID	Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	Group
1	None ▼
2	None ▼
3	None ▼
4	None ▼
5	None ▼
6	None ▼
7	None ▼
8	None ▼

Apply Cancel

The following table describes the labels in this screen.

Table 37 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

15.5 Link Aggregation Control Protocol

Click **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Section 15.2 on page 133](#) for more information on dynamic link aggregation.

Figure 64 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

Link Aggregation Control Protocol Link Aggregation Setting

Active ☐

System Priority

Group ID	LACP Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	LACP Timeout
*	30 seconds
1	30 seconds
2	30 seconds
3	30 seconds
4	30 seconds
5	30 seconds
6	30 seconds
7	30 seconds
8	30 seconds

Apply Cancel

The following table describes the labels in this screen.

Table 38 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.

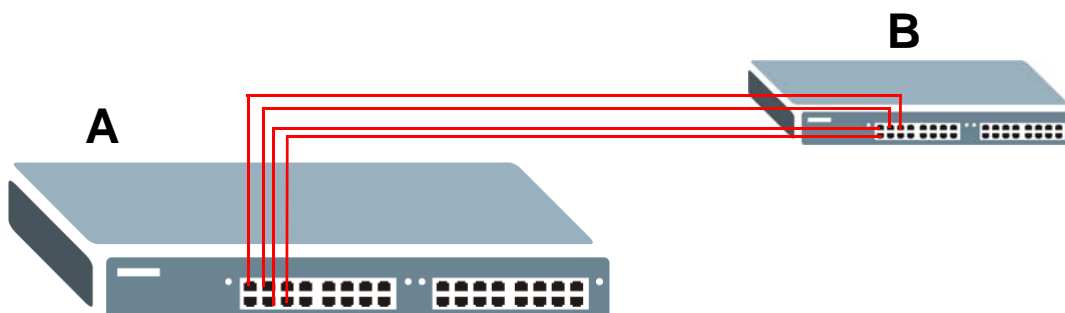
Table 38 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
LACP Timeout	<p>Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible.</p> <p>Select either 1 second or 30 seconds.</p>
Apply	<p>Click Apply to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

15.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

- 1 Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 65 Trunking Example - Physical Connections

- 2 Configure static trunking** - Click **Advanced Application > Link Aggregation > Link Aggregation Setting**. In this screen activate trunking group **T1** and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 66 Trunking Example - Configuration Screen

Link Aggregation Setting

Status LACP

Group ID	Active
T1	<input checked="" type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>

Port	Group
1	None
2	T1
3	T1
4	T1
5	T1
6	None
7	None
8	None

Apply

Cancel

Your trunk group 1 (T1) configuration is now complete; you do not need to go to any additional screens.

Port Authentication

This chapter describes the IEEE 802.1x and MAC authentication methods.

16.1 Port Authentication Overview

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following methods for port authentication:

- **IEEE 802.1x²** - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See [Section 23.1.2 on page 186](#) for more information on configuring your RADIUS server settings.

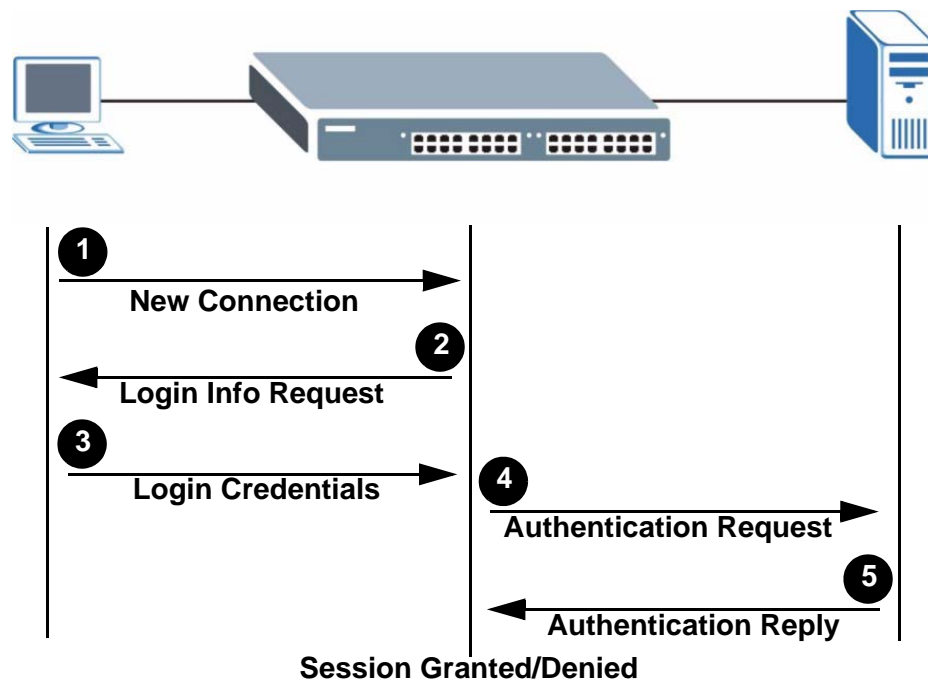


If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication first. If a user fails to authenticate via the IEEE 802.1x method, then access to the port is denied.

16.1.1 IEEE 802.1x Authentication

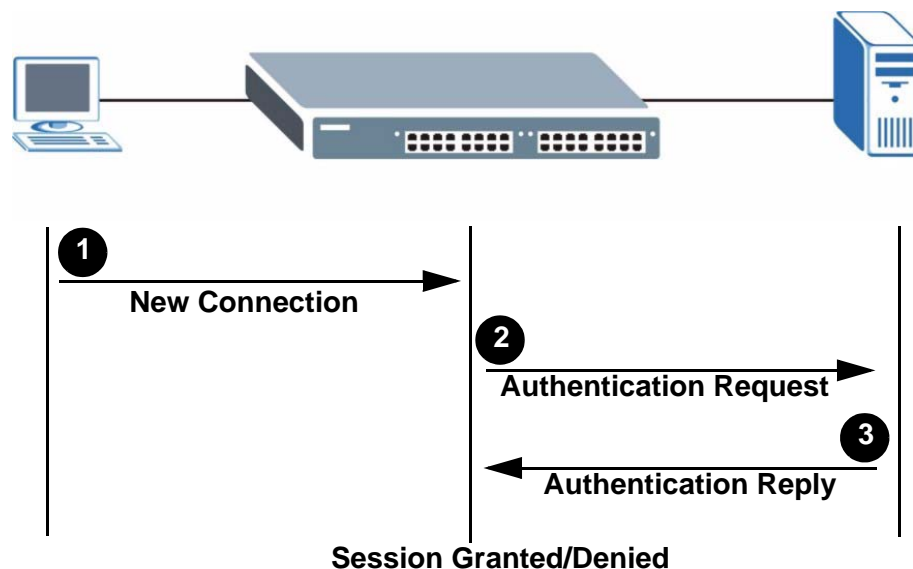
The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

-
2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

Figure 67 IEEE 802.1x Authentication Process

16.1.2 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 68 MAC Authentication Process

16.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method(s) you want to use (both on the Switch and the port(s)) then configure the RADIUS server settings in the **Auth and Acct > Radius Server Setup** screen.

Click **Advanced Application > Port Authentication** in the navigation panel to display the screen as shown.

Figure 69 Advanced Application > Port Authentication



16.2.1 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 70 Advanced Application > Port Authentication > 802.1x

Port	Active	Reauthentication	Reauthentication Timer
*	<input type="checkbox"/>	On	seconds
1	<input type="checkbox"/>	On	3600 seconds
2	<input type="checkbox"/>	On	3600 seconds
3	<input type="checkbox"/>	On	3600 seconds
4	<input type="checkbox"/>	On	3600 seconds
5	<input type="checkbox"/>	On	3600 seconds
6	<input type="checkbox"/>	On	3600 seconds
7	<input type="checkbox"/>	On	3600 seconds
8	<input type="checkbox"/>	On	3600 seconds

The following table describes the labels in this screen.

Table 39 Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.2 Activate MAC Authentication

Use this screen to activate MAC authentication. In the **Port Authentication** screen click **MAC Authentication** to display the configuration screen as shown.

Figure 71 Advanced Application > Port Authentication > MAC Authentication

MAC Authentication **Port Authentication**

Active ☐

Name Prefix

Password

Timeout

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 40 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	<p>Select this check box to permit MAC authentication on the Switch.</p> <p>Note: You must first enable MAC authentication on the Switch before configuring it on each port.</p>
Name Prefix	<p>Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters.</p> <p>If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.</p>
Password	<p>Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.</p>
Timeout	<p>Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds.</p> <p>When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, then this entry will not be deleted from the MAC address table.</p> <p>Note: If the Aging Time in the Switch Setup screen is set to a lower value, then it supersedes this setting. See Section 7.5 on page 81.</p>
Port	This field displays the port number.

Table 40 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
*	<p>Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this checkbox to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.2 Port Security Setup

Click **Advanced Application > Port Security** in the navigation panel to display the screen as shown.

Figure 72 Advanced Application > Port Security

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>

Apply Cancel

The following table describes the labels in this screen.

Table 41 Advanced Application > Port Security

LABEL	DESCRIPTION
Active	Select this option to enable port security on the Switch.
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	<p>Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped.</p> <p>Clear this check box to disable the port security feature. The Switch forwards all packets on this port.</p>
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16384". "0" means this feature is disabled.

Table 41 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Classifier

This chapter introduces and shows you how to configure the packet classifier on the Switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 19 on page 157](#) to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 19 on page 157](#).

Click **Advanced Application > Classifier** in the navigation panel to display the configuration screen as shown.

Figure 73 Advanced Application > Classifier

Classifier

Active ☐

Name

Packet Format **All**

Layer 2

VLAN ☒ Any ☐

Priority ☒ Any ☐

Ethernet Type ☒ All ☐ Others (Hex)

Source MAC Address ☒ Any ☐ MAC : : : : :

Port ☒ Any ☐

Destination MAC Address ☒ Any ☐ MAC : : : : :

Layer 3

DSCP ☒ Any ☐

IP Protocol ☒ All ☐ Establish Only ☐ Others (Dec)

Source IP Address / Address Prefix 0.0.0.0 /

Socket Number ☒ Any ☐

Destination IP Address / Address Prefix 0.0.0.0 /

Socket Number ☒ Any ☐

Add Cancel Clear

The following table describes the labels in this screen.

Table 42 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are All , 802.3 tagged , 802.3 untagged , Ethernet II tagged and Ethernet II untagged . A value of 802.3 indicates that the packets are formatted according to the IEEE 802.3 standards. A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
VLAN	Select Any to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select Any to classify traffic from any priority level or select the second option and specify a priority level in the field provided.

Table 42 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
Ethernet Type	Select an Ethernet type or select Other and enter the Ethernet type number in hexadecimal value. Refer to Table 44 on page 154 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (Any).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select Other and enter the protocol number in decimal value. Refer to Table 45 on page 155 for more information. You may select Establish Only for TCP protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click Add to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.



When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 74 Advanced Application > Classifier: Summary Table

Index	Active	Name	Rule	Delete
1	Yes	Example	EtherType = IP; SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>
<div> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> </div>				

The following table describes the labels in this screen.

Table 43 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 44 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

Table 45 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 75 Classifier: Example

Classifier

Active ☒

Name

Packet Format

Layer 2

VLAN ☒ Any ☐

Priority ☒ Any ☐

Ethernet Type ☒ All ☐ Others (Hex)

Source ☒ MAC Address ☐ MAC : : : : :

☐ Port ☒

Destination ☒ MAC Address ☐ MAC : : : : :

Layer 3

DSCP ☒ Any ☐

IP Protocol ☒ All ☐ Others (Dec) ☐ Establish Only

Source /

Socket Number ☒ Any ☐

Destination /

Socket Number ☒ Any ☐

Policy Rule

This chapter shows you how to configure policy rules.

19.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 18 on page 151](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 18.2 on page 151](#) for more information.

Click **Advanced Applications > Policy Rule** in the navigation panel to display the screen as shown.

Figure 76 Advanced Application > Policy Rule

Policy

Active ☐

Name

Classifier(s)

Parameters

General

VLAN ID

Egress Port

Outgoing packet format for Egress port ☒ Tag ☐ Untag

Priority

DSCP

TOS

Metering

Bandwidth Kbps

Out-of-Profile

DSCP

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1 priority

☐ Send the packet to priority queue

☐ Replace the 802.1 priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1 priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

☐ Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port

☐ Set the packet's VLAN ID

Metering

☐ Enable

Out-of-profile action

☐ Drop the packet

☐ Change the DSCP value

☐ Set Out-Drop Precedence

☐ Do not drop the matching frame previously marked for dropping

Add Cancel Clear

The following table describes the labels in this screen.

Table 46 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Type the number of an outgoing port.
Outgoing packet format for Egress port	Select Tag to add the specified VID to packets on the specified outgoing port. Otherwise, select Untag .
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select No change to forward the packets. Select Discard the packet to drop the packets. Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before.
Priority	Select No change to keep the priority setting of the frames. Select Set the packet's 802.1 priority to replace the packet's 802.1 priority field with the value you set in the Priority field. Select Send the packet to priority queue to put the packets in the designated queue. Select Replace the 802.1 priority field with the IP TOS value to replace the packet's 802.1 priority field with the value you set in the TOS field.
Diffserv	Select No change to keep the TOS and/or DSCP fields in the packets. Select Set the packet's TOS field to set the TOS field with the value you configure in the TOS field. Select Replace the IP TOS with the 802.1 priority value to replace the TOS field with the value you configure in the Priority field. Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.

Table 46 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Outgoing	Select Send the packet to the mirror port to send the packet to the mirror port. Select Send the packet to the egress port to send the packet to the egress port. Select Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port. Select Set the packet's VLAN ID to set the VLAN ID of the packet with the value you configure in the VLAN ID field.
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP value to replace the DSCP field with the value specified in the Out of profile DSCP field. Select Set Out-Drop Precedence to mark out-of-profile traffic and drop it when network is congested. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Add	Click Add to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 77 Advanced Application > Policy Rule: Summary Table

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example;	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 47 Advanced Application > Policy Rule: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 18.4 on page 155](#)).

Figure 78 Policy Example

Policy

Active ☒

Name

Classifier(s)

Parameters

VLAN ID

Egress Port

Outgoing packet format for Egress port ☒ Tag ☐ Untag

Priority

DSCP

TOS

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1 priority

☐ Send the packet to priority queue

☐ Replace the 802.1 priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1 priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

☐ Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port

☐ Set the packet's VLAN ID

Metering

☐ Enable

Out-of-profile action

☒ Drop the packet

☐ Change the DSCP value

☐ Set Out-Drop Precedence

☐ Do not drop the matching frame previously marked for dropping

Add Cancel Clear

Queuing Method

This chapter introduces the queuing methods supported.

20.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment in Switch Setup** and **802.1p Priority in Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

20.1.1 Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

20.1.2 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

20.2 Configuring Queuing

Click **Advanced Application, Queuing Method** in the navigation panel.

Figure 79 Queuing Method

Port	Method	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
2	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
3	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
4	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
5	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
6	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
7	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
8	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
9	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
10	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
11	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
12	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8

Apply Cancel

The following table describes the labels in this screen.

Table 48 Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select SPQ (Strict Priority Queuing) or WRR (Weighted Round Robin). Strict Priority Queuing (SPQ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Round Robin Scheduling (WRR) services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Q0–Q7 Weight	When you select WRR , enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN

21.1 VLAN Stacking Overview

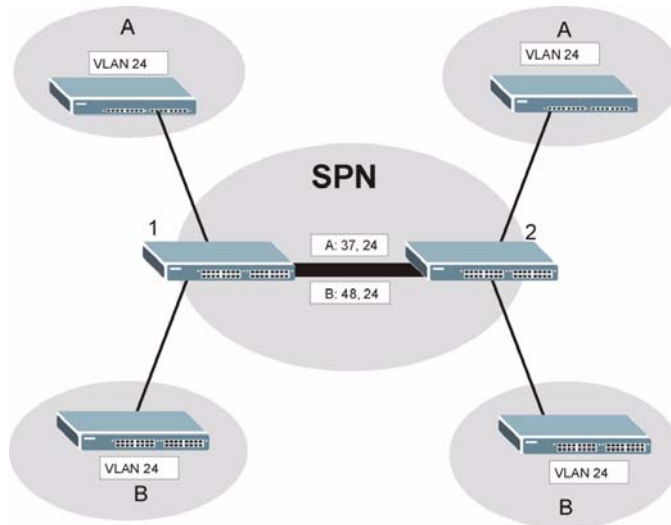
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider’s customers may require a range of VLANs to handle multiple applications. A service provider’s customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

21.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider’s Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 80 VLAN Stacking Example

21.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.



Static VLAN Tx Tagging MUST be disabled on a port where you choose Normal or Access Port.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).



Static VLAN Tx Tagging MUST be enabled on a port where you choose Tunnel Port.

21.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 49 VLAN Tag Format

Type	Priority	VID
------	----------	-----

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

21.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

Table 50 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/Etype	Data	FCS	Double-tagged frame

Table 51 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame

Table 51 802.1Q Frame

(SP)TPID	(Service Provider) Tag Protocol Identifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

21.4 Configuring VLAN Stacking

Click **Advanced Applications > VLAN Stacking** to display the screen as shown.

Figure 81 Advanced Application > VLAN Stacking

Port	Role	SPVID	Priority
*	Access Port		0
1	Access Port	1	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0

The following table describes the labels in this screen.

Table 52 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
SP TPID	SP TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose 0x8100 or 0x9100 from the drop-down list box or select Others and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the Others text field.
Port	The port number identifies the port you are configuring.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>

Table 52 Advanced Application > VLAN Stacking (continued)

LABEL	DESCRIPTION
Role	<p>Select Normal to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in SPVID and Priority are ignored.</p> <p>Note: The Normal option is only supported on the GS-4012F model.</p> <p>Select Access Port to have the Switch add the SP TPID tag to all incoming frames received on this port. Select Access Port for ingress ports at the edge of the service provider's network.</p> <p>Select Tunnel Port (available for Gigabit ports only) for egress ports at the edge of the service provider's network.</p> <p>In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.</p>
SPVID	<p>SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 8 on page 91 for more background information on VLAN ID.</p>
Priority	<p>On the Switch, configure priority level of inner IEEE 802.1Q tag in the Port Setup screen. "0" is the lowest priority level and "7" is the highest.</p>
Apply	<p>Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

Multicast

This chapter shows you how to configure various multicast features.

22.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

22.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

22.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

22.1.3 IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

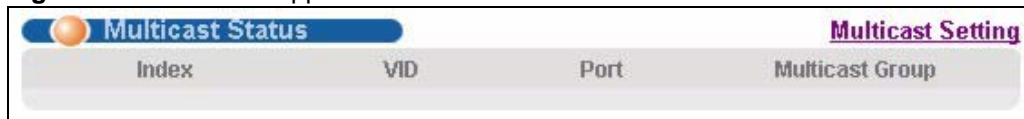
22.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

22.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See [Section 22.1 on page 171](#) for more information on multicasting.

Figure 82 Advanced Application > Multicast



Index	VID	Port	Multicast Group
-------	-----	------	-----------------

The following table describes the labels in this screen.

Table 53 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

22.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See [Section 22.1 on page 171](#) for more information on multicasting.

Figure 83 Advanced Application > Multicast > Multicast Setting

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="checkbox"/>	<input type="checkbox"/>		Default	Auto
1	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
2	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
3	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
4	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
5	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
6	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
7	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
8	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto

The following table describes the labels in this screen.

Table 54 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select Active to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.

Table 54 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Reserved Multicast Group	Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA web site for more information. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the Multicast > Multicast Setting > IGMP Filtering Profile screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

22.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See [Section 22.1.4 on page 172](#) for more information on IGMP Snooping VLAN.

Figure 84 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

The following table describes the labels in this screen.

Table 55 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	<p>Select auto to have the Switch learn multicast group membership information of any VLANs automatically.</p> <p>Select fixed to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below.</p> <p>In either auto or fixed mode, the Switch can learn up to 16 VLANs (including up to three VLANs you configured in the MVR screen). For example, if you have configured one multicast VLAN in the MVR screen, you can only specify up to 15 VLANs in this screen.</p> <p>The Switch drops any IGMP control messages which do not belong to these 16 VLANs.</p> <p>Note: You must also enable IGMP snooping in the Multicast Setting screen first.</p>
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	<p>Enter the ID of a static VLAN; the valid range is between 1 and 4094.</p> <p>Note: You cannot configure the same VLAN ID as in the MVR screen.</p>
Add	Click Add to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click this to clear the fields.

Table 55 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

22.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications > Multicast > Multicast Setting > IGMP Filtering Profile** link to display the screen as shown.

Figure 85 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

The following table describes the labels in this screen.

Table 56 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the Start Address and End Address fields.

Table 56 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Add	Click Add to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

22.6 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1, 2 and 3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 86 MVR Network Example

22.6.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

22.6.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

22.6.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 87 MVR Multicast Television Example



22.7 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications > Multicast > Multicast Setting > MVR** link to display the screen as shown next.



You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.



Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 88 Advanced Application > Multicast > Multicast Setting > MVR

The following table describes the related labels in this screen.

Table 57 Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are Dynamic and Compatible . Select Dynamic to send IGMP reports to all MVR source ports in the multicast VLAN. Select Compatible to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.

Table 57 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

22.8 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.



A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 89 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

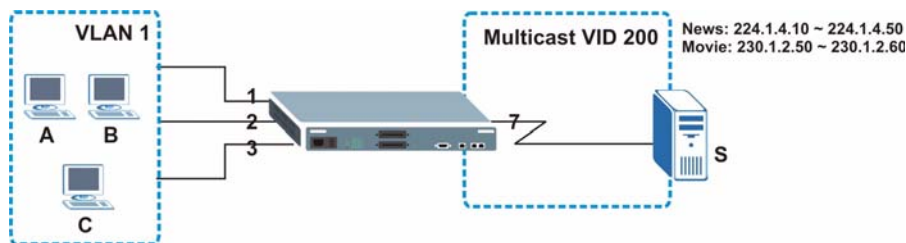
The following table describes the labels in this screen.

Table 58 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the MVR screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 22.1.1 on page 171 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group. Refer to Section 22.1.1 on page 171 for more information on IP multicast addresses.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select Delete Group and click Delete to remove the selected entry(ies) from the table.
Cancel	Select Cancel to clear the checkbox(es) in the table.

22.8.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN are able to receive the traffic.

Figure 90 MVR Configuration Example

To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 91 MVR Configuration Example

Port	Source Port	Receiver Port	None	Tagging
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 92 MVR Group Configuration Example

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>

Figure 93 MVR Group Configuration Example

Group Configuration

MVR

Multicast VLAN ID

200

Name	Start Address	End Address
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

Add

Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				<input type="checkbox"/>	
	Movie	230.1.2.50	230.1.2.60		<input type="checkbox"/>
	News	224.1.4.10	224.1.4.50		<input type="checkbox"/>

Delete

Cancel

Authentication & Accounting

This chapter describes how to configure authentication and accounting settings on the Switch.

23.1 Authentication, Authorization and Accounting

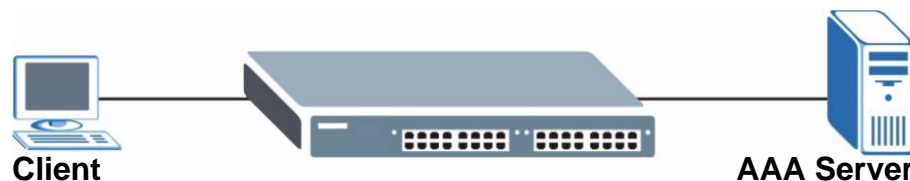
Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see [Section 23.1.2 on page 186](#)) and TACACS+ (Terminal Access Controller Access-Control System Plus, see [Section 23.1.2 on page 186](#)) as external authentication, authorization and accounting servers.

Figure 94 AAA Server



23.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See [Chapter 35 on page 279](#)).

23.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 59 RADIUS vs TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

23.2 Authentication and Accounting Screens

To enable authentication, accounting or both on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority and accounting settings.

Click **Advanced Application > Auth and Acct** in the navigation panel to display the screen as shown.

Figure 95 Advanced Application > Auth and Acct



23.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [Section 23.1.2 on page 186](#) for more information on RADIUS servers and [Section 23.3 on page 194](#) for RADIUS attributes utilized by the authentication and accounting features on the Switch. . Click on the **RADIUS Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 96 Advanced Application > Auth and Acct > RADIUS Server Setup

RADIUS Server Setup Auth and Acct

Authentication Server

Mode: index-priority

Timeout: 30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1812		<input type="checkbox"/>
2	0.0.0.0	1812		<input type="checkbox"/>

Apply Cancel

Accounting Server

Timeout: 30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1813		<input type="checkbox"/>
2	0.0.0.0	1813		<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 60 Advanced Application > Auth and Acct > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	<p>This field is only valid if you configure multiple RADIUS servers.</p> <p>Select index-priority and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server.</p> <p>Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.</p>
Timeout	<p>Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server.</p> <p>If you are using index-priority for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.</p>
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.

Table 60 Advanced Application > Auth and Acct > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for accounting is 1813 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See [Section 23.1.2 on page 186](#) for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 97 Advanced Application > Auth and Acct > TACACS+ Server Setup

TACACS+ Server Setup Auth and Acct

Authentication Server

Mode: index-priority

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		<input type="checkbox"/>
2	0.0.0.0	49		<input type="checkbox"/>

Apply Cancel

Accounting Server

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		<input type="checkbox"/>
2	0.0.0.0	49		<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 61 Advanced Application > Auth and Acct > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	<p>This field is only valid if you configure multiple TACACS+ servers.</p> <p>Select index-priority and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server.</p> <p>Select round-robin to alternate between the TACACS+ servers that it sends authentication requests to.</p>
Timeout	<p>Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server.</p> <p>If you are using index-priority for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.</p>
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is 49 . You need not change this value unless your network administrator instructs you to do so.

Table 61 Advanced Application > Auth and Acct > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for accounting is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.2.3 Authentication and Accounting Setup

Use this screen to configure authentication and accounting settings on the Switch. Click on the **Auth and Acct Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 98 Advanced Application > Auth and Acct > Auth and Acct Setup

Auth and Acct Setup Auth and Acct

Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

Accounting

Update Period: 0 minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	<input type="checkbox"/>	<input type="checkbox"/>	-	radius	-
Exec	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Dot1x	<input type="checkbox"/>	<input type="checkbox"/>	start-stop	radius	-
Commands	<input type="checkbox"/>	<input type="checkbox"/>	stop-only	tacacs+	0

Apply Cancel

The following table describes the labels in this screen.

Table 62 Advanced Application > Auth and Acct > Auth and Acct Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	<p>These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management).</p> <p>Configure the access privilege of accounts via commands (See Section 45.7 on page 328) for local authentication. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first Method 1, then Method 2 and finally Method 3). You must configure the settings in the Method 1 field. If you want the Switch to check other sources for access privilege level specify them in Method 2 and Method 3 fields.</p> <p>Select local to have the Switch check the access privilege configured for local authentication.</p> <p>Select radius or tacacs+ to have the Switch check the access privilege via the external servers.</p>

Table 62 Advanced Application > Auth and Acct > Auth and Acct Setup (continued)

LABEL	DESCRIPTION
Login	<p>These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management).</p> <p>Configure the local user accounts in the Access Control > Logins screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first Method 1, then Method 2 and finally Method 3). You must configure the settings in the Method 1 field. If you want the Switch to check other sources for administrator accounts, specify them in Method 2 and Method 3 fields.</p> <p>Select local to have the Switch check the administrator accounts configured in the Access Control > Logins screen.</p> <p>Select radius to have the Switch check the administrator accounts configured in the RADIUS Server Setup screen.</p> <p>Select tacacs+ to have the Switch check the administrator accounts configured in the TACACS+ Server Setup screen.</p>
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec or Dot1x entries.
Type	<p>The Switch supports the following types of events to be sent to the accounting server(s):</p> <ul style="list-style-type: none"> • System - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • Exec - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • Dot1x - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • Commands - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	<p>Select this to have the Switch send accounting information to all configured accounting servers at the same time.</p> <p>If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.</p>
Mode	<p>The Switch supports two modes of recording login events. Select:</p> <ul style="list-style-type: none"> • start-stop - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the Update Period), and when a user ends a session. • stop-only - to have the Switch send information to the accounting server only when a user ends a session.
Method	<p>Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events.</p> <p>TACACS+ is the only method for recording Commands type of event.</p>
Privilege	<p>This field is only configurable for Commands type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.</p>

Table 62 Advanced Application > Auth and Acct > Auth and Acct Setup (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See [Section 45.7 on page 328](#) for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID:** An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type:** A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data:** A value you want to assign to the setting.



Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 63 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 1 Vendor-data = ingress rate (Kbps in decimal format)

Table 63 Supported VSAs

FUNCTION	ATTRIBUTE
Egress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 2 Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = 890 Vendor-Type = 3 Vendor-Data = " shell:priv-lvl=N " or Vendor-ID = 9 (CISCO) Vendor-Type = 1 (CISCO-AVPAIR) Vendor-Data = " shell:priv-lvl=N " where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

23.2.4.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 64 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = VLAN(13) Tunnel-Medium-Type = 802(6) Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch.

23.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This appendix lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

23.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name
 - the format of the User-Name attribute is **\$enab#\$**, where # is the privilege level (1=14)
 User-Password
 NAS-Identifier
 NAS-IP-Address

23.3.1.2 Attributes Used to Login Users

User-Name
 User-Password
 NAS-Identifier
 NAS-IP-Address

23.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name
 NAS-Identifier
 NAS-IP-Address
 NAS-Port
 NAS-Port-Type
 - This value is set to **Ethernet(15)** on the Switch.
 Calling-Station-Id
 Frame-MTU
 EAP-Message
 State
 Message-Authenticator

23.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address
 NAS-Identifier
 Acct-Status-Type
 Acct-Session-ID
 - The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)
 Acct-Delay-Time

23.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 65 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

Table 66 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Calling-Station-Id	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

23.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 67 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-IP-Address	Y	Y	Y
NAS-Port	Y	Y	Y
Class	Y	Y	Y
Called-Station-Id	Y	Y	Y
Calling-Station-Id	Y	Y	Y
NAS-Identifier	Y	Y	Y

Table 67 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
NAS-Port-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Input-Octets		Y	Y
Acct-Output-Octets		Y	Y
Acct-Session-Time		Y	Y
Acct-Input-Packets		Y	Y
Acct-Output-Packets		Y	Y
Acct-Terminate-Cause			Y
Acct-Input-Gigawords		Y	Y
Acct-Output-Gigawords		Y	Y

IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

24.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

24.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

24.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.



The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

24.1.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 99 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

24.1.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See [Chapter 33 on page 259](#) for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings ([Chapter 33 on page 259](#)).

24.1.1.4 Configuring DHCP Snooping

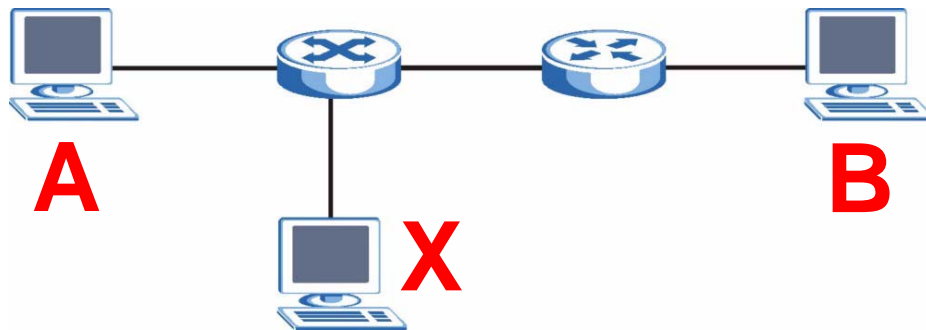
Follow these steps to configure DHCP snooping on the Switch.

- 1 Enable DHCP snooping on the Switch.
- 2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
- 3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4 Configure static bindings.

24.1.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 100 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

24.1.2.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters ([Chapter 10 on page 107](#)).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

24.1.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

24.1.2.3 Syslog

The Switch can send syslog messages to the specified syslog server ([Chapter 38 on page 305](#)) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

24.1.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

- 1 Configure DHCP snooping. See [Section 24.1.1.4 on page 201](#).




It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

- 2 Enable ARP inspection on each VLAN.
- 3 Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

24.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 101 IP Source Guard



Index	Mac Address	IP Address	Lease	Type	VID	Port
1	a1:12:12:12:12:01	172.23.37.222	infinity	static	1	18

The following table describes the labels in this screen.

Table 68 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
Mac Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, 2d3h4m5s means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays infinity if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. static: This binding was learned from information provided manually by an administrator. dhcp-snooping: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

24.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 102 IP Source Guard Static Binding

IP Source Guard Static Binding IPSG

MAC Address : : : : :

IP Address

VLAN

Port ☐ ☒ Any

Add Cancel Clear

Index	MAC Address	IP Address	Lease	Type	VLAN	Port	Delete
Delete Cancel							

The following table describes the labels in this screen.

Table 69 IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select Any .
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. static : This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click Delete to remove the specified entry.
Cancel	Click this to clear the Delete check boxes above.

24.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 103 DHCP Snooping

DHCP Snooping

Configure

IPSG

Database Status

Description		Status
Agent URL		
Write delay timer	300	seconds
Abort timer	300	seconds
Agent running		
Delay timer expiry	Not Running	
Abort timer expiry	Not Running	
Last succeeded time		
Last failed time	None	
Last failed reason	No failure recorded	
Times		
Total attempts	0	
Startup failures	0	
Successful transfers	0	
Failed transfers	0	
Successful reads	0	
Failed reads	0	
Successful writes	0	
Failed writes	0	

Database detail

Description	Status
First successful access	None
Last ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0
Last ignored time	None
Total ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0

The following table describes the labels in this screen.

Table 70 DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the DHCP Snooping Configure screen. See Section 24.5 on page 208 .
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. none : The Switch is not accessing the DHCP snooping database. read : The Switch is loading dynamic bindings from the DHCP snooping database. write : The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays Not Running if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays Not Running if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.

Table 70 DHCP Snooping (continued)

LABEL	DESCRIPTION
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See Chapter 45 on page 325 .
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See Chapter 45 on page 325 .
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

24.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 104 DHCP Snooping Configure

The following table describes the labels in this screen.

Table 71 DHCP Snooping Configure

LABEL	DESCRIPTION
Active	<p>Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports.</p> <p>Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.</p>
DHCP Vlan	<p>Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN.</p> <p>Note: You have to enable DHCP snooping on the DHCP VLAN too.</p> <p>You can enable Option82 in the DHCP Snooping VLAN Configure screen (Section 24.5.2 on page 211) to help the DHCP servers distinguish between DHCP requests from different VLAN.</p> <p>Select Disable if you do not want the Switch to forward DHCP packets to a specific VLAN.</p>

Table 71 DHCP Snooping Configure (continued)

LABEL	DESCRIPTION
Database	If Timeout interval is greater than Write delay interval , it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: tftp://{domain name or IP address}/directory, if applicable/file name ; for example, tftp://192.168.10.1/database.txt .
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click Renew if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in Agent URL . When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the Binding collisions counter in the DHCP Snooping screen (Section 24.4 on page 205).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.



The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 105 DHCP Snooping Port Configure

Port	Server Trusted state	Rate (pps)
*	Untrusted	
1	Untrusted	0
2	Untrusted	0
3	Untrusted	0
4	Untrusted	0
5	Untrusted	0
6	Untrusted	0
7	Untrusted	0
8	Untrusted	0

Apply Cancel

The following table describes the labels in this screen.

Table 72 DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	<p>Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted).</p> <p>Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.</p> <p>Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations:</p> <ul style="list-style-type: none"> The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). The source MAC address and source IP address in the packet do not match any of the current bindings. The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information ([Chapter 33 on page 259](#)) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 106 DHCP Snooping VLAN Configure

The following table describes the labels in this screen.

Table 73 DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select Yes to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen. See Section 24.5 on page 208 .
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the General Setup screen. See Chapter 7 on page 77 . You can specify the DHCP VLAN in the DHCP Snooping Configure screen. See Section 24.5 on page 208 .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 107 ARP Inspection Status

Index	Mac Address	VID	Port	Expiry (sec)	Reason	Delete
*	-	-	-	-	-	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 74 ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
Mac Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (Delete).
Reason	This field displays the reason the ARP packet was discarded. MAC+VLAN: The MAC address and VLAN ID were not in the binding table. IP: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. Port: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this, and click Delete to remove the specified entry.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the Delete check boxes above.

24.6.1 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 108 ARP Inspection VLAN Status

ARP Inspection VLAN Status [Status](#)

Show VLAN range

☒ Enabled VLAN

☐ Selected VLAN

Start VID

End VID

VID	Received	Request	Reply	Forwarded	Dropped

The following table describes the labels in this screen.

Table 75 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (Start VID) and the highest VLAN ID (End VID) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

24.6.2 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 109 ARP Inspection Log Status

ARP Inspection Log Status [Status](#)

Clearing log status table

Total number of logs = 0

Index	Port	VID	Sender Mac	Sender IP	Num Pkts	Reason	Time
-------	------	-----	------------	-----------	----------	--------	------

The following table describes the labels in this screen.

Table 76 ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click Apply to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called overflow with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender Mac	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the ARP Inspection Configure screen. See Section 24.7 on page 215 .
Reason	<p>This field displays the reason the log message was generated.</p> <p>dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID.</p> <p>static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID.</p> <p>deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID.</p> <p>dhcp permit: An ARP packet was forwarded because it matched a dynamic binding.</p> <p>static permit: An ARP packet was forwarded because it matched a static binding.</p> <p>In the ARP Inspection VLAN Configure screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 24.7.2 on page 217.</p>
Time	This field displays when the log message was generated.

24.7 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 110 ARP Inspection Configure

The screenshot shows the 'ARP Inspection Configure' interface. It includes a title bar with the page name and three tabs: 'Port', 'VLAN', and 'ARP Inspection'. The 'ARP Inspection' tab is selected. Below the tabs, there is a section for 'Active' with a checkbox. The next section is 'Filter Aging Time' with a 'Filter aging time' field set to '300' and the unit 'seconds'. The final section is 'Log Profile' with three fields: 'Log buffer size' set to '32' (entries), 'Syslog rate' set to '5' (entries), and 'Log interval' set to '1' (seconds). At the bottom are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 77 ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified Syslog rate and Log interval . If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click Clearing log status table in the ARP Inspection Log Status screen to clear the log and reset this counter. See Section 24.6.2 on page 213 .

Table 77 ARP Inspection Configure (continued)

LABEL	DESCRIPTION
Syslog rate	<p>Enter the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the Log Interval. You must configure the syslog server (Chapter 38 on page 305) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server.</p> <p>The relationship between Syslog rate and Log interval is illustrated in the following examples:</p> <ul style="list-style-type: none"> 4 invalid ARP packets per second, Syslog rate is 5, Log interval is 1: the Switch sends 4 syslog messages every second. 6 invalid ARP packets per second, Syslog rate is 5, Log interval is 2: the Switch sends 10 syslog messages every 2 seconds.
Log interval	<p>Enter how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See Syslog rate for an example of the relationship between Syslog rate and Log interval.</p>
Apply	<p>Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click this to reset the values in this screen to their last-saved values.</p>

24.7.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 111 ARP Inspection Port Configure

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted		
1	Untrusted	15	1
2	Untrusted	15	1
3	Untrusted	15	1
4	Untrusted	15	1
5	Untrusted	15	1
6	Untrusted	15	1
7	Untrusted	15	1
8	Untrusted	15	1

Apply Cancel

The following table describes the labels in this screen.

Table 78 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: <ul style="list-style-type: none"> The sender's information in the ARP packet does not match any of the current bindings. The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	These settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.7.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 112 ARP Inspection VLAN Configure

ARP Inspection VLAN Configure [Configure](#)

VLAN Start VID End VID

Apply

VID	Enabled	Log
*	No	None

Apply Cancel

The following table describes the labels in this screen.

Table 79 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select Yes to enable ARP inspection on the VLAN. Select No to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. None: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. Deny: The Switch generates log messages when it discards an ARP packet from the VLAN. Permit: The Switch generates log messages when it forwards an ARP packet from the VLAN. All: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

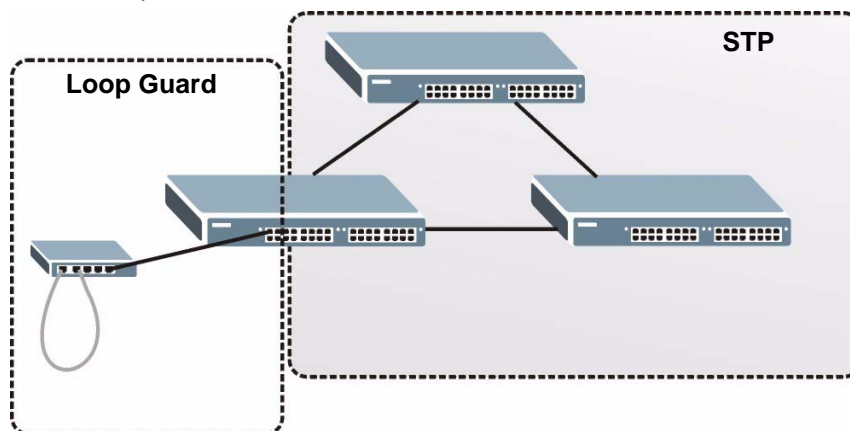
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

25.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network.

Figure 113 Loop Guard vs STP



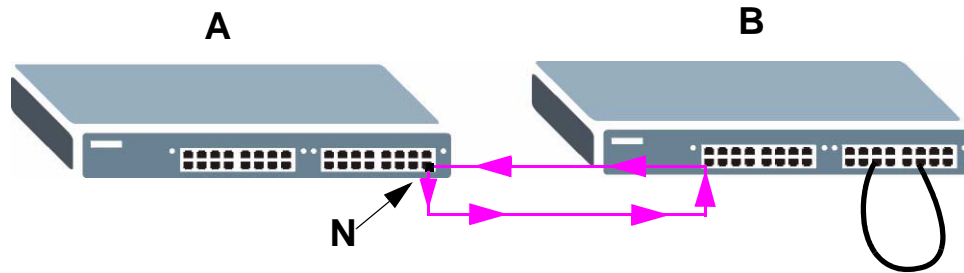
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

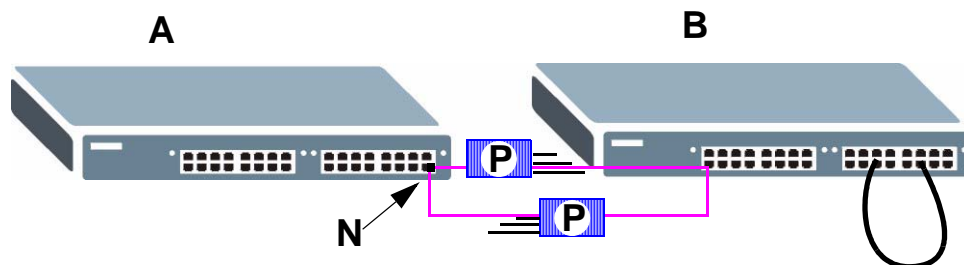
Figure 114 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

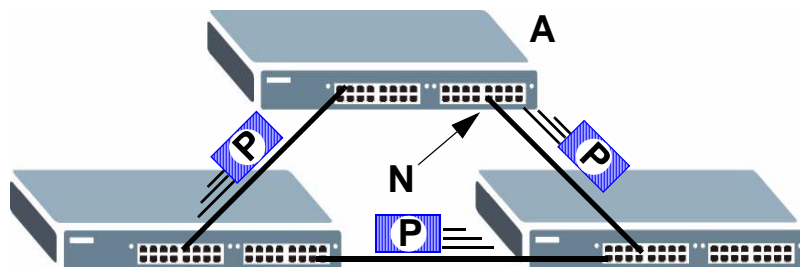
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 115 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 116 Loop Guard - Network Loop





After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see [Section 7.7 on page 85](#)) or via commands (see [Section 45.12.4 on page 368](#)).

25.2 Loop Guard Setup

Click **Advanced Application > Loop Guard** in the navigation panel to display the screen as shown.



The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 117 Advanced Application > Loop Guard

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 80 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 80 Advanced Application > Loop Guard (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

PART IV

IP Application

Static Route (225)

RIP (227)

OSPF (229)

IGMP (241)

DVMRP (245)

IP Multicast (249)

Differentiated Services (251)

DHCP (259)

VRRP (267)

Static Route

This chapter shows you how to configure static routes.

26.1 Configuring Static Routing

Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **IP Application**, **Static Routing** in the navigation panel to display the screen as shown.

Figure 118 Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	255.255.0.0	192.168.1.2	2	<input type="checkbox"/>

The following table describes the related labels you use to create a static route.

Table 81 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.

Table 81 Static Routing (continued)

LABEL	DESCRIPTION
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

This chapter shows you how to configure RIP (Routing Information Protocol).

27.1 RIP Overview

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the Switch will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **Incoming** - the Switch will not send any RIP packets but will accept all RIP packets received.
- **Outgoing** - the Switch will send out RIP packets but will not accept any RIP packets received.
- **None** - the Switch will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Switch sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

27.2 Configuring RIP

Click **IP Application**, **RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 7.6 on page 83](#)).

Figure 119 RIP

The following table describes the labels in this screen.

Table 82 RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the Switch.
Index	This field displays the index number of an IP interface.
Network	This field displays the IP interface configured on the Switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are Outgoing , Incoming , Both and None .
Version	Select the RIP version from the drop-down list box. Choices are RIP-1 , RIP-2B and RIP-2M .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring the fields again.

This chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF.

28.1 OSPF Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

OSPF offers some advantages over traditional vector-space routing protocols (such as RIP). The following table summarizes some of the major differences between OSPF and RIP.

Table 83 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metrics	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

28.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS, is not a transit area since there is only one connection to the stub area.

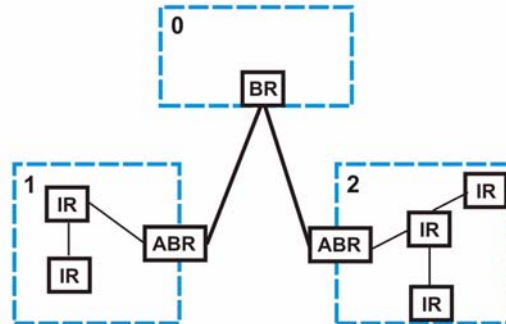
The following table describes the four classes of OSPF routers.

Table 84 OSPF: Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASes.

The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

Figure 120 OSPF Network Example



28.1.2 How OSPF Works

Layer 3 devices exchange routing information to build synchronized link state database within the same AS or area. They do this by exchanging Hello messages to confirm which neighbor (layer 3) devices exist and then they exchange database descriptions (DDs) to create the link state database. The link state database is constantly updated through LSAs (Link State Advertisements).

The link state database contains records of router IDs, their associated links and path costs. Each device can then use the link state database and Dijkstra algorithm to compute the least cost paths to network destinations.

28.1.3 Interfaces and Virtual Links

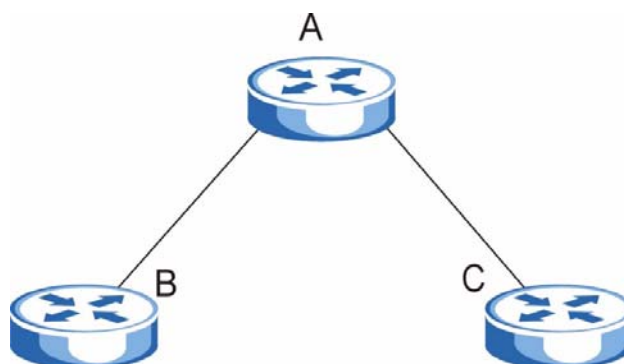
An OSPF interface is a link between a layer 3 device and an OSPF network. An interface has state information, an IP address and subnet mask associated with it. When you configure an OSPF interface, you first set an interface to transmit OSPF traffic and add the interface to an area.

You can configure a virtual link to establish/maintain connectivity between a non-backbone area and the backbone. The virtual link must be configured on both layer 3 devices in the non-backbone area and the backbone.

28.1.4 OSPF and Router Elections

The OSPF protocol provides for automatic election of Designated Router (DR) and Backup Designated Router (BDR) on network segments. The DR and BDR keep track of link state updates in their area and make sure LSAs are sent to the rest of the network.

In most cases the default DR/BDR election is fine, but in some situations it must be controlled. In the following figure only router **A** has direct connectivity with all the other routers on the network segment. Routers **B** and **C** do not have a direct connection with each other. Therefore they should not be allowed to become DR or BDR. Only router **A** should become the DR.

Figure 121 OSPF Router Election Example

You can assign a priority to an interface which determines whether this router will be elected to be a DR or BDR. The router with the highest priority becomes the DR, while a router with a priority of 0 does not participate in router elections. In [Figure 121 on page 231](#) you can assign a priority of 0 to routers **B** and **C**, thereby ensuring they do not become DR or BDR and assign a priority of 1 to router **A** to make sure that it does become the DR.

28.1.5 Configuring OSPF

To configure OSPF on the Switch, do the following tasks

- 1 Enable OSPF
- 2 Create OSPF areas
- 3 Create and associate interface(s) to an area
- 4 Create virtual links to maintain backbone connectivity.

28.2 OSPF Status

Use this screen to view current OSPF status. Click **IP Application, OSPF** in the navigation panel to display the screen as shown next. See [Section 28.1 on page 229](#) for more information on OSPF.

Figure 122 OSPF Status

OSPF Status Configuration

OSPF: Running

Interface:

```
VLINK0 is down, line protocol is down
  OSPF is enabled, but not running on this interface
swif2 is up, line protocol is up
  Internet Address 192.168.1.10/24, Area 192.168.1.1
  Router ID 192.168.1.10, Network Type BROADCAST, Cost: 15
  Transmit Delay is 1 sec, State Backup, Priority 1
```

Neighbor:

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/DR	00:00:34	192.168.1.1	swif2:192.168.

Link State Database:

```
OSPF Router with ID (192.168.1.10)
  Router Link States (Area 0.0.0.0)
Link ID      ADV Router    Age  Seq#    CkSum  Link count
```

Poll Interval(s) Set Interval Stop

The following table describes the labels in this screen.

Table 85 OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated (Running) or not (Down).
Interface	The text box displays the OSPF status of the interface(s) on the Switch.
Neighbor	The text box displays the status of the neighboring router participating in the OSPF network.
Link State Database	The text box displays information in the link state database which contains data in the LSAs.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to end OSPF status polling.

The following table describes some common output fields.

Table 86 OSPF Status: Common Output Fields

FIELD	DESCRIPTION
Interface	
Internet Address	This field displays the IP address and subnet bits of an IP routing domain.
Area	This field displays the area ID.
Router ID	This field displays the unique ID of the Switch.
Transmit Delay	This field displays the transmission delay in seconds.

Table 86 OSPF Status: Common Output Fields (continued)

FIELD	DESCRIPTION
State	This field displays the state of the Switch (backup or DR (designated router)).
Priority	This field displays the priority of the Switch. This number is used in the designated router election.
Designated Router	This field displays the router ID of the designated router.
Backup Designated Router	This field displays the router ID of a backup designated router.
Time Intervals Configured	This field displays the time intervals (in seconds) configured.
Neighbor Count	This field displays the number of neighbor routers.
Adjacent Neighbor Count	This field displays the number of neighbor router(s) that is adjacent to the Switch.
Neighbor	
Neighbor ID	This field displays the router ID of the neighbor.
Pri	This field displays the priority of the neighbor. This number is used in the designated router election.
State	This field displays the state of the neighbor (backup or DR (designated router)).
Dead Time	This field displays the dead time in seconds.
Address	This field displays the IP address of a neighbor.
Interface	This field displays the MAC address of a device.
Link State Database	
Link ID	This field displays the ID of a router or subnet.
ADV Router	This field displays the IP address of the layer-3 device that sends the LSAs.
Age	This field displays the time (in seconds) since the last LSA was sent.
Seq #	This field displays the link sequence number of the LSA.
Checksum	This field displays the checksum value of the LSA.
Link Count	This field displays the number of links in the LSA.

28.3 OSPF Configuration

Use this screen to activate OSPF and set general settings. Click **IP Application**, **OSPF** and the **Configuration** link to display the **OSPF Configuration** screen. See [Section 28.1 on page 229](#) for more information on OSPF.

OSPF Configuration: Activating and General Settings

The follow table describes the related labels in this screen.

Table 87 OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Active	OSPF is disabled by default. Select this option to enable it.
Router ID	Router ID uniquely identifies the Switch in an OSPF. Enter a unique ID (that uses the format of an IP address in dotted decimal notation) for the Switch.
Redistribute Route	Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP and Static) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learn through the selected protocol.
Type	Select 1 for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the AB boundary router to the external metrics. Select 2 for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, the external cost of the AB boundary router is used in path decision to a destination.
Metric Value	Enter a route cost (between 0 and 16777214).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the above fields again.

28.4 Configure OSPF Areas

To ensure that the Switch receives only routing information from a trusted layer 3 devices, activate authentication. The OSPF supports three authentication methods:

- None – no authentication is used.
- Simple – authenticate link state updates using an 8 printable ASCII character password.
- MD5 – authenticate link state updates using a 16 printable ASCII character password.

To configure an area, set the related fields in the **OSPF Configuration** screen.

Figure 123 OSPF Configuration: Area Setup

OSPF Configuration Interface Virtual Link Status

Active ☐

Router ID

Redistribute Route	Active	Type	Metric value
RIP	<input checked="" type="checkbox"/>	1	15
Static	<input checked="" type="checkbox"/>	1	15

Apply Cancel

Name

Area ID

Authentication None

Stub Network ☐

No Summary ☐

Default route cost

Add Cancel Clear

Index	Name	Area ID	Authentication	Stub Network	Delete
-------	------	---------	----------------	--------------	--------

Delete Cancel

The following table describes the related labels in this screen.

Table 88 OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Enter a 32-bit ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. A value of 0.0.0.0 indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the Switch.
Authentication	Select an authentication method (Simple or MD5) to activate authentication. Select None (default) to disable authentication. Usually interface(s) and virtual interface(s) should use the same authentication method as the associated area. If interface(s) and virtual interface(s) use different authentication methods than the associated area, the authentication methods are based on the interface(s) and virtual interface(s) settings.

Table 88 OSPF Configuration: Area Setup (continued)

LABEL	DESCRIPTION
Stub Network	Select this option to set the area as a stub area. If you enter 0.0.0.0 in the Area ID field, the settings in the Stub Area fields are ignored.
No Summary	Select this option to set the Switch to not send/receive LSAs.
Default Route Cost	Specify a cost (between 0 and 16777214) used to add a default route into a stub area for routes which are external to an OSPF domain. If you do not set a route cost, no default route is added.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the above fields again.
Clear	Click Clear to set the above fields back to the factory defaults.

28.4.1 View OSPF Area Information Table

The bottom of the **OSPF Configuration** screen displays a summary table of all the OSPF areas you have configured.

Figure 124 OSPF Configuration: Summary Table

Index	Name	Area ID	Authentication	Stub Network	Delete
1	Example	192.168.1.1	None	No	<input type="checkbox"/>
<div> Delete Cancel </div>					

The following table describes the related labels in this screen.

Table 89 OSPF Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Name	This field displays the descriptive name of an area.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. An area ID of 0.0.0.0 indicates the backbone.
Authentication	This field displays the authentication method used (None , Simple or MD5).
Stub Network	This field displays whether an area is a stub network (Yes) or not (No).
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

28.5 Configuring OSPF Interfaces

To configure an OSPF interface, first create an IP routing domain in the **IP Setup** screen (see [Section 7.6 on page 83](#) for more information). Once you create an IP routing domain, an OSPF interface entry is automatically created. See [Section 28.1 on page 229](#) for more information on OSPF.

In the **OSPF Configuration** screen, click **Interface** to display the **OSPF Interface** screen.

Figure 125 OSPF Interface

Index	Network	Area ID	Authentication	Key ID	Cost	Priority	Delete
1	192.168.1.1/24	192.168.1.1	None	1	15	111	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 90 OSPF Interface

LABEL	DESCRIPTION
Network	Select an IP interface.
Area ID	Select the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Authentication	<p>Note: OSPF Interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are Same-as-Area, None (default), Simple and MD5.</p> <p>To participate in an OSPF network, you must set the authentication method and/or password the same as the associated area.</p> <p>Select Same-as-Area to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select None to disable authentication. This is the default setting.</p> <p>Select Simple and set the Key field to authenticate OSPF packets transmitted through this interface using simple password authentication.</p> <p>Select MD5 and set the Key ID and Key fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authentication you want to use.
Key	<p>When you select Simple in the Authentication field, enter a password eight-character long. Characters after the eighth character will be ignored.</p> <p>When you select MD5 in the Authentication field, enter a password 16-character long.</p>
Cost	The interface cost is used for calculating the routing table. Enter a number between 0 and 65535. The default interface cost is 15.

Table 90 OSPF Interface (continued)

LABEL	DESCRIPTION
Priority	The priority you assign to the interface is used in router elections to decide which router is going to be the Designated Router (DR) or the Backup Designated Router (BDR). You can assign a number between 0 and 255. A priority of 0 means that the router will not participate in router elections.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the above fields again.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number for an interface.
Network	This field displays the IP interface information.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Authentication	This field displays the authentication method used (Same-as-Area , None , Simple or MD5).
Key ID	When the Authentication field displays MD5 , this field displays the identification number of the key used.
Cost	This field displays the interface cost used for calculating the routing table.
Priority	This field displays the priority for this OSPF interface.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to start configuring the above fields again.

28.6 OSPF Virtual-Links

Configure and view virtual link settings in this screen. See [Section 28.1 on page 229](#) for more information on OSPF.

In the **OSPF Configuration** screen, click **Virtual-Link** to display the screen as shown next.

Figure 126 OSPF Virtual Link

The following table describes the related labels in this screen.

Table 91 OSPF Virtual-Link

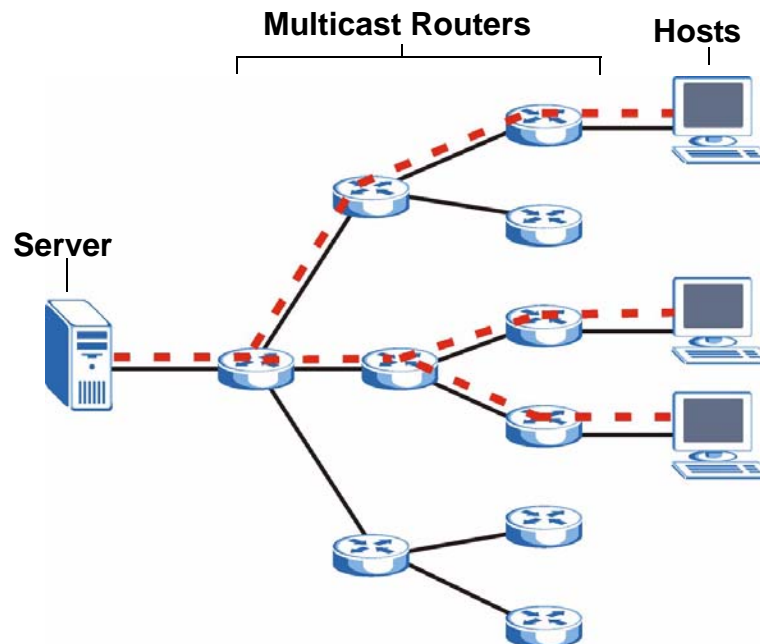
LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Select the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Peer Router ID	Enter the ID of a peer border router.
Authentication	<p>Note: Virtual interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are Same-as-Area, None (default), Simple and MD5.</p> <p>To exchange OSPF packets with peer border router, you must set the authentication method and/or password the same as the peer border router.</p> <p>Select Same-as-Area to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select None to disable authentication. This is the default setting.</p> <p>Select Simple to authenticate OSPF packets transmitted through this interface using a simple password.</p> <p>Select MD5 to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authentication you want to use.
Key	<p>When you select Simple in the Authentication field, enter a password eight-character long.</p> <p>When you select MD5 in the Authentication field, enter a password 16-character long.</p>
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the above fields again.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays an index number of an entry.
Name	This field displays a descriptive name of a virtual link.
Peer Router ID	This field displays the ID (that uses the format of an IP address in dotted decimal notation) of a peer border router.
Authentication	This field displays the authentication method used (Same-as-Area , None , Simple or MD5).
Key ID	When the Authentication field displays MD5 , this field displays the identification number of the key used.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

This chapter shows you how to configure the Switch as a multicast router.

29.1 IGMP Overview

IP multicast is an IETF standard for distributing data to multiple recipients. The following figure shows a multicast session and the relationship between a multicast server, multicast routers and multicast hosts. A multicast server transmits multicast packets and multicast routers forward multicast packets to multicast hosts.

Figure 127 IP Multicast



A host can decide to join or leave a multicast group at any time. A host can also be a member of more than one multicast group. Multicast groups are identified by IP addresses in the Class D range (224.0.0.0 to 239.255.255.255). A multicast server sends packets addressed to a particular multicast group (multicast IP address).

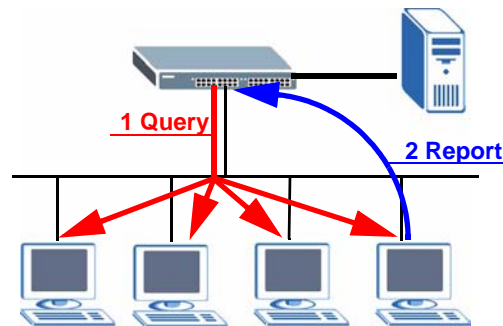
IGMP (Internet Group Management Protocol) is used by multicast hosts to indicate their multicast group membership to multicast routers. Multicast routers can also use IGMP to periodically check if multicast hosts still want to receive transmission from a multicast server. In other words, multicast routers check if any hosts on their network are still members of a specific multicast group.

The Switch supports IGMP version 1 (**IGMP-v1**), version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively. At start up, the Switch queries all directly connected networks to gather group membership. After that, the Switch periodically updates this information.

29.1.1 How IGMP Works

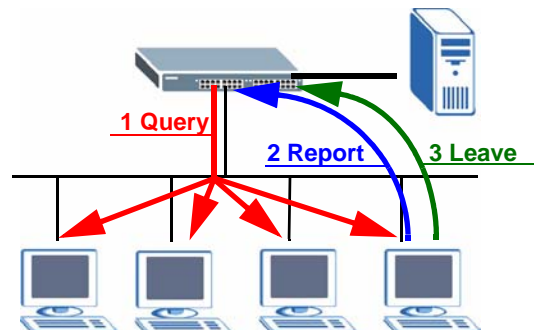
This section describes how IGMP works and the changes it has gone through from version 1 to version 3. IGMP version 1 defines how a multicast router checks to see if any multicast hosts are part of a multicast group. It checks for group membership by sending out an IGMP Query packet. Hosts that are members of a multicast group reply with an IGMP Report packet. This is also referred to as a join group request. The multicast router then keeps a list of all networks that have members of this multicast group and forwards multicast traffic to that network.

Figure 128 IGMP Version 1 Example



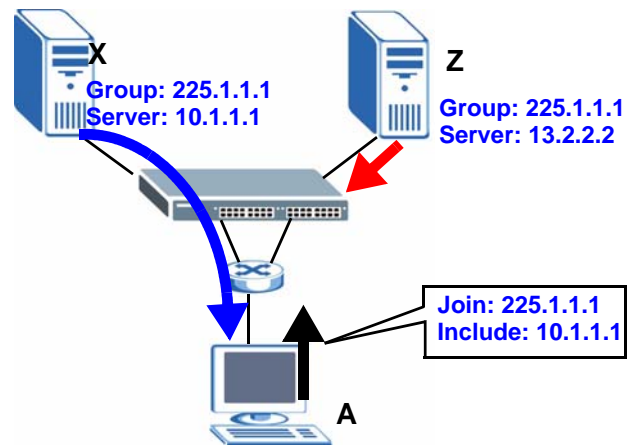
The main difference in IGMP version 2 is that it provides a mechanism for a multicast group member to notify a multicast router that it is leaving a multicast group. The multicast router then sends a group-specific IGMP query to check if there are any members remaining in that group. If the multicast router does not receive an IGMP report from any members, it stops sending multicast traffic to that group. This change helps shorten the leave convergence time. In other words, the amount of time that a multicast router believes that there are group members on a particular network. This in turn helps reduce the amount of multicast traffic going through the multicast router.

Figure 129 IGMP Version 2 Example



IGMP version 3 allows a multicast host to join a multicast group and specify from which source (multicast server) it wants to receive multicast packets. Alternatively, a multicast host can specify from which multicast servers it does not want to receive multicast packets. In the following figure multicast server **X** (IP address **10.1.1.1**) and multicast server **Z** (IP address **13.2.2.2**) both send multicast traffic to the same multicast group identified by the multicast IP address **225.1.1.1**. In IGMP version 3 multicast host **A** can join multicast group **225.1.1.1** and specify that it only wants to receive multicast packets from server **X**.

Figure 130 IGMP Version 3 Example



29.2 Port-based IGMP

The Switch sends IGMP Query packets to all ports. The Switch then listens for IGMP Report packets, and it records which port the messages came from. It then delivers multicast traffic to only those ports from which it received a request to join a multicast group.

29.3 Configuring IGMP

Click **IP Application**, **IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 7.6 on page 83](#)).

Figure 131 IP Application > IGMP

The screenshot shows the IGMP configuration interface. At the top, there's a section for 'Active' with a checkbox and 'Unknown Multicast Frame' with radio buttons for 'Flooding' (selected) and 'Drop'. Below this is a table with columns 'Index', 'Network', and 'Version'. The table contains one entry with Index 1 and Network 172.23.37.203/24, where the Version is set to 'None'. At the bottom are 'Apply' and 'Cancel' buttons.

Index	Network	Version
1	172.23.37.203/24	None

The following table describes the labels in this screen.

Table 92 IP Application > IGMP

LABEL	DESCRIPTION
Active	<p>Select this check box to enable IGMP on the Switch.</p> <p>Note: You cannot enable both IGMP snooping and IGMP at the same time. Refer to Section 22.3 on page 172 for more information on IGMP snooping.</p>
Unknown Multicast Frame	<p>Specify the action to perform when the Switch receives an unknown multicast frame. Unknown multicast frames are addressed to multicast groups for which the Switch has not recorded any group members. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.</p>
Index	<p>This field displays an index number of an entry.</p>
Network	<p>This field displays the IP domain configured on the Switch.</p> <p>Refer to Section 7.6 on page 83 for more information on configuring IP domains.</p>
Version	<p>Select an IGMP version from the drop-down list box. Choices are IGMP-v1, IGMP-v2, IGMP-v3 and None.</p> <p>Generally, if you want to enable IGMP on the Switch, you should choose IGMP-v3 as it is compatible with older versions. Choose an earlier version of IGMP (IGMP-v2 or IGMP-v1) if the multicast hosts on your network can not recognize IGMP version 3 or version 2 Query messages.</p>
Apply	<p>Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

This chapter introduces DVMRP and tells you how to configure it.

30.1 DVMRP Overview

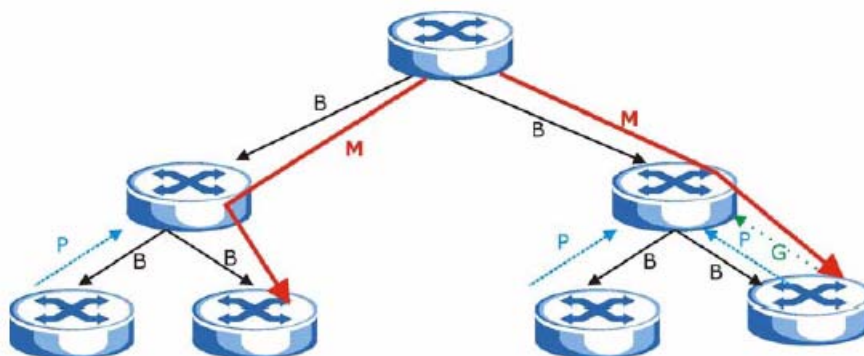
DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). This DVMRP implementation is based on draft-ietf-idmr-dvmrp-v3-10. DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol. The DVMRP metric is a hop count of 32.

IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in [Figure 134 on page 247](#).

30.2 How DVMRP Works

DVMRP uses the Reverse Path Multicasting (RPM) algorithm to generate an IP Multicast delivery tree. Multicast packets are forwarded along these multicast tree branches. DVMRP dynamically learns host membership information using Internet Group Management Protocol (IGMP). The trees are updated dynamically to track the membership of individual groups.

- 1 Initially an advertisement multicast packet is broadcast (“B” in the following figure).
- 2 DVMRP-enabled Layer 3 devices that do not have any hosts in their networks that belong to this multicast group send back a prune message (“P”).
- 3 If hosts later join the multicast group, a graft message (“G”) to undo the prune is sent to the parent.
- 4 The final multicast (“M”) after pruning and grafting is shown in the next figure.

Figure 132 How DVMRP Works

30.2.1 DVMRP Terminology

DVMRP probes are used to discover other DVMRP Neighbors on a network.

DVMRP reports are used to exchange DVMRP source routing information. These packets are used to build the DVMRP multicast routing table that is used to build source trees and also perform Reverse Path Forwarding (RPF) checks on incoming multicast packets. RPF checks prevent duplicate packets being filtered when loops exist in the network topology.

DVMRP prunes trim the multicast delivery tree(s). DVMRP grafts attach a branch back onto the multicast delivery tree.

30.3 Configuring DVMRP

Configure DVMRP on the Switch when you wish it to act as a multicast router (“mrouter”). Click **IP Application**, **DVMRP** in the navigation panel to display the screen as shown.

Figure 133 DVMRP

Index	Network	VID	Active
1	10.10.10.1/24	2	<input type="checkbox"/>
2	192.168.1.1/24	1	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 93 DVMRP

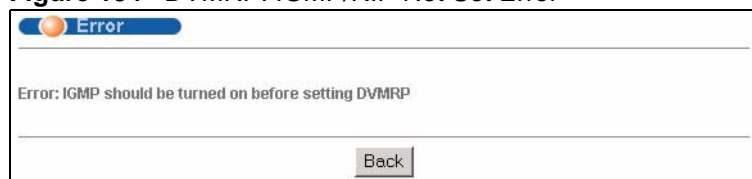
LABEL	DESCRIPTION
Active	Select Active to enable DVMRP on the Switch. You should do this if you want the Switch to act as a multicast router.
Threshold	Threshold is the maximum time to live (TTL) value. TTL is used to limit the scope of multicasting. You should reduce this value if you do not wish to flood Layer 3 devices many hops away with multicast traffic. This applies only to multicast traffic this Switch sends out.

Table 93 DVMRP (continued)

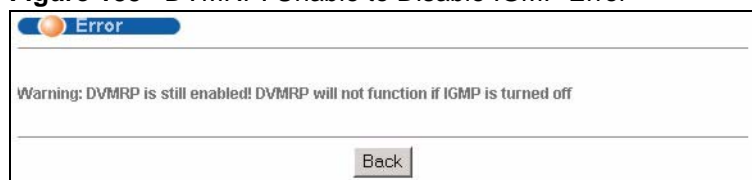
LABEL	DESCRIPTION
Index	Index is the DVMRP configuration for the IP routing domain defined under Network . The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the Switch. See Section 7.6 on page 83 for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in IP Setup .
VID	DVMRP cannot be enabled on the same VLAN group across different IP routing domains, that is, you cannot have duplicate VIDs for different DVMRP configurations (see Figure 136 on page 247).
Active	Select Active to enable DVMRP on this IP routing domain.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this part of the screen afresh.

30.3.1 DVMRP Configuration Error Messages

You must have IGMP/RIP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

Figure 134 DVMRP: IGMP/RIP Not Set Error

When you disable IGMP, but DVMRP is still active you also see another warning screen.

Figure 135 DVMRP: Unable to Disable IGMP Error

Each IP routing domain DVMRP configuration must be in a different VLAN group; otherwise you see the following screen.

Figure 136 DVMRP: Duplicate VID Error Message

30.4 Default DVMRP Timer Values

The following are some default DVMRP timer values.

Table 94 DVMRP: Default Timer Values

DVMRP FIELD	DEFAULT VALUE
Probe interval	10 sec
Report interval	35 sec
Route expiration time	140 sec
Prune lifetime	Variable (less than two hours)
Prune retransmission time	3 sec with exponential back off
Graft retransmission time	5 sec with exponential back off

IP Multicast

This chapter shows you how to configure the **IP Multicast** screen.

31.1 IP Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (one sender to one recipient) or Broadcast (one sender to everybody on the network). IP Multicast is a third way to deliver IP packets to a group of hosts on the network - not everybody.

You can configure the Switch to untag (remove the VLAN tags from) IP multicast packets that the Switch forwards. This allows the Switch to send packets to Ethernet devices that are not VLAN-aware.

31.2 Configuring Multicast

Click **IP Application** and **IP Multicast** in the navigation panel to display the screen as shown next.

Figure 137 IP Multicast

Port	IP Multicast Egress Untag Vlan ID
*	
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

Apply Cancel

The following table describes the labels in this screen.

Table 95 IP Multicast

LABEL	DESCRIPTION
Port	This read-only field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
IP Multicast Egress Untag Vlan ID	The Switch removes the VLAN tag from IP multicast packets belonging to the specified VLAN before transmission on this port. Enter a VLAN group ID in this field. Enter 0 to set the Switch not to remove any VLAN tags from the packets.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

32.1 DiffServ Overview

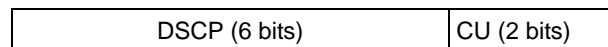
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

32.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 138 DiffServ: Differentiated Service Field



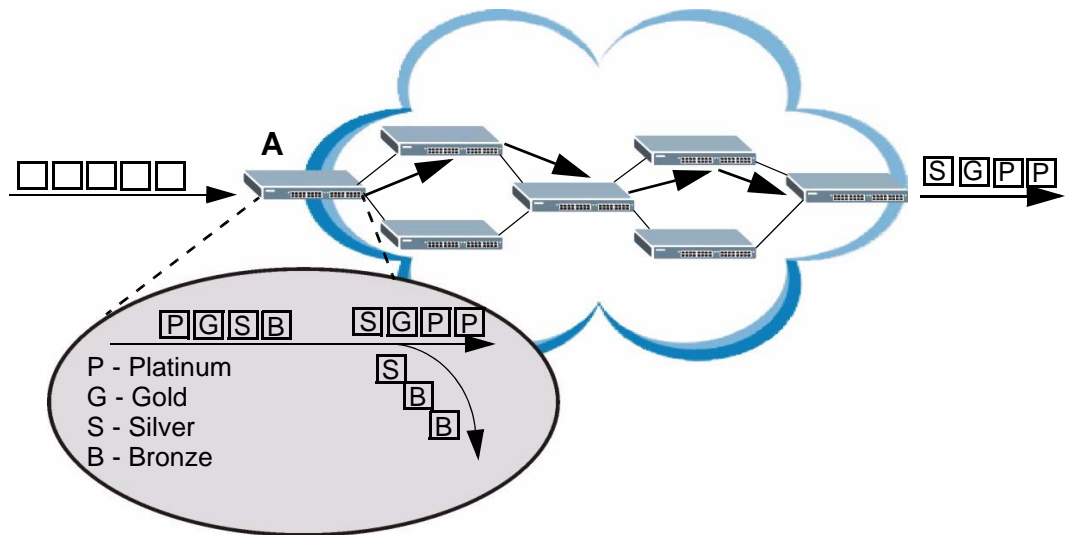
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

32.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in [Figure 139](#)) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum, Gold, Silver, Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 139 DiffServ Network



32.2 Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.

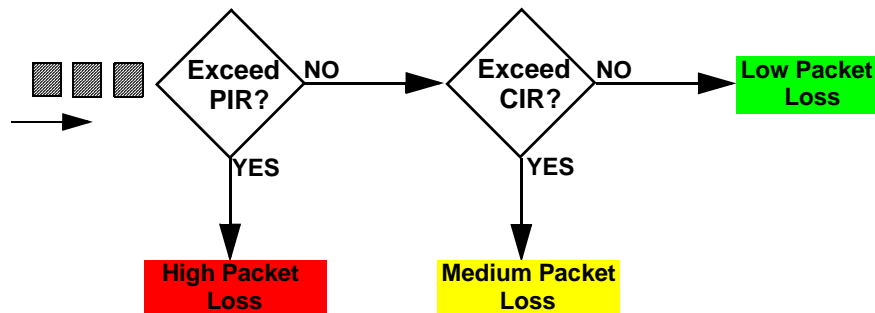
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

32.2.1 TRTCM - Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 140 TRTCM - Color-blind Mode

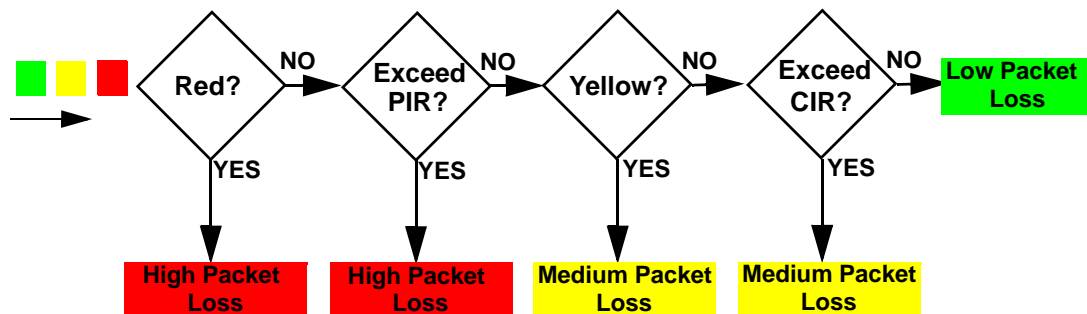


32.2.2 TRTCM - Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (high packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level are they evaluated against the CIR.

Figure 141 TRTCM - Color-aware Mode



32.3 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 142 IP Application > DiffServ

Port	Active
*	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 96 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select Active to enable DiffServ on the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

32.3.1 Configuring 2-Rate 3 Color Marker Settings

Use this screen to configure TRTCM settings. Click the **2-rate 3 Color Marker** link in the **DiffServ** screen to display the screen as shown next.



You cannot enable both TRTCM and Bandwidth Control at the same time.

Figure 143 IP Application > DiffServ > 2-rate 3 Color Marker

Port	Active	Commit Rate	Peak Rate	green	yellow	red
*	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="text"/> Kbps	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following table describes the labels in this screen.

Table 97 IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings. Note: You must also activate DiffServ on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select color-blind to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select color-aware to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.
Commit Rate	Specify the Commit Information Rate (CIR) for this port.
Peak Rate	Specify the Peak Information Rate (PIR) for this port.

Table 97 IP Application > DiffServ > 2-rate 3 Color Marker (continued)

LABEL	DESCRIPTION
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.
green	Specify the DSCP value to use for packets with low packet loss priority.
yellow	Specify the DSCP value to use for packets with medium packet loss priority.
red	Specify the DSCP value to use for packets with high packet loss priority.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

32.4 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

Table 98 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

32.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 144 IP Application > DiffServ > DSCP Setting

The screenshot shows the 'DSCP Setting' configuration page under 'Diffserv'. The title is 'DSCP Setting' with a sub-header 'DSCP to 802.1p Mapping'. The page displays a table with 64 entries, each consisting of a DSCP value (0-63) and a corresponding IEEE 802.1p value (0-7). The values are currently set to 0 for DSCP 0-7, 1 for 8-15, 2 for 16-23, 3 for 24-31, 4 for 32-39, 5 for 40-47, 6 for 48-55, and 7 for 56-63. At the bottom, there are 'Apply' and 'Cancel' buttons.

DSCP	802.1p	DSCP	802.1p	DSCP	802.1p	DSCP	802.1p
0	0	8	1	16	2	24	3
1	0	9	1	17	2	25	3
2	0	10	1	18	2	26	3
3	0	11	1	19	2	27	3
4	0	12	1	20	2	28	3
5	0	13	1	21	2	29	3
6	0	14	1	22	2	30	3
7	0	15	1	23	2	31	3
8	1	16	2	24	3	32	4
9	1	17	2	25	3	33	4
10	1	18	2	26	3	34	4
11	1	19	2	27	3	35	4
12	1	20	2	28	3	36	4
13	1	21	2	29	3	37	4
14	1	22	2	30	3	38	4
15	1	23	2	31	3	39	4
16	2	24	3	32	4	40	5
17	2	25	3	33	4	41	5
18	2	26	3	34	4	42	5
19	2	27	3	35	4	43	5
20	2	28	3	36	4	44	5
21	2	29	3	37	4	45	5
22	2	30	3	38	4	46	5
23	2	31	3	39	4	47	5
24	3	32	4	40	5	48	6
25	3	33	4	41	5	49	6
26	3	34	4	42	5	50	6
27	3	35	4	43	5	51	6
28	3	36	4	44	5	52	6
29	3	37	4	45	5	53	6
30	3	38	4	46	5	54	6
31	3	39	4	47	5	55	6
32	4	40	5	48	6	56	7
33	4	41	5	49	6	57	7
34	4	42	5	50	6	58	7
35	4	43	5	51	6	59	7
36	4	44	5	52	6	60	7
37	4	45	5	53	6	61	7
38	4	46	5	54	6	62	7
39	4	47	5	55	6	63	7

The following table describes the labels in this screen.

Table 99 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

This chapter shows you how to configure the DHCP feature.

33.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the Switch as a DHCP server or a DHCP relay agent. When configured as a server, the Switch provides the TCP/IP configuration for the clients. If you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP server or relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

33.1.1 DHCP Modes

The Switch can be configured as a DHCP server or DHCP relay agent.

- If you configure the Switch as a DHCP server, it will maintain the pool of IP addresses along with subnet masks, DNS server and default gateway information and distribute them to your LAN computers.
- If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

33.1.2 DHCP Configuration Options

The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured as a DHCP server for one VLAN and at the same time the Switch can be configured to relay DHCP requests for clients in another VLAN.

33.2 DHCP Status

Click **IP Application > DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 145 IP Application > DHCP Status

DHCP Status			
Global			
Server Status:			
Index	VID	Server Status	IP Pool Size
1	2	192.168.2.100	66
Relay Status			
Relay Mode		VLAN:1-3	

The following table describes the labels in this screen.

Table 100 IP Application > DHCP Status

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	This is the index number.
VID	This field displays the VLAN ID for which the Switch is a DHCP server.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the number of IP addresses that can be assigned to clients.
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: <ul style="list-style-type: none"> • None - if the Switch is not configured as a DHCP relay agent. • Global - if the Switch is configured as a DHCP relay agent only. • VLAN - followed by a VLAN ID if it is configured as a relay agent for specific VLAN(s).

33.3 DHCP Server Status Detail

Click **IP Application > DHCP** in the navigation panel and then click an existing index number of a DHCP server configuration to view the screen as shown. Use this screen to view details regarding DHCP server settings configured on the Switch.

Figure 146 IP Application > DHCP > DHCP Server Status Detail

Server Status Detail

DHCP Status

Start IP Address	192.168.1.33
End IP Address	192.168.1.62
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary DNS Server	192.168.5.1
Secondary DNS Server	192.168.5.2

Address Leases

Index	IP Address	Timer	Hardware Address	Hostname
-------	------------	-------	------------------	----------

The following table describes the labels in this screen.

Table 101 IP Application > DHCP Server Status Detail

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Address Leases	This section displays information about the IP addresses this DHCP server issued to clients.
Index	This field displays a sequential number for each DHCP request handled by the Switch.
IP Address	This is the IP address issued to a DHCP client.
Timer	This field displays the time remaining before the DHCP client has to renew its IP address.
Hardware Address	This field displays the MAC address of the DHCP client. It may also display SELF OCCUPIED ADDRESS , if the IP address cannot be used for DHCP because it is already assigned to the Switch itself.
Hostname	This field displays the system name of the client.

33.4 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

33.4.1 DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The **DHCP Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings > General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

Table 102 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 32 bytes) This optional, read-only field is set according to system name set in Basic Settings > General Setup .

33.4.2 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 147 IP Application > DHCP > Global

The following table describes the labels in this screen.

Table 103 IP Application > DHCP > Global

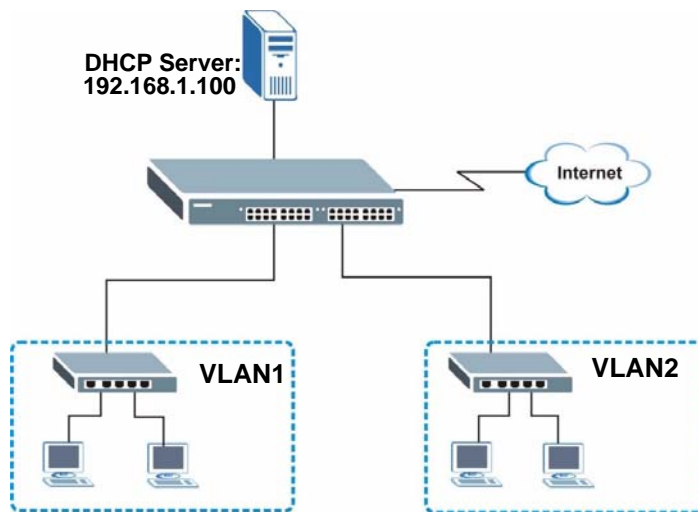
LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the Option 82 check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.

Table 103 IP Application > DHCP > Global (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

33.4.3 Global DHCP Relay Configuration Example

The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 148 Global DHCP Relay Network Example

Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 149 DHCP Relay Configuration Example

The screenshot shows the 'DHCP Relay' configuration window. It has a 'Status' tab and an 'Active' checkbox which is checked. Below this, there are three rows for 'Remote DHCP Server' with IP addresses: 192.168.1.100, 0.0.0.0, and 0.0.0.0. Under 'Relay Agent Information', the 'Option 82' checkbox is checked, and the 'Information' field contains 'GS-4012F'. At the bottom are 'Apply' and 'Cancel' buttons.

DHCP Relay		Status
Active	<input checked="" type="checkbox"/>	
Remote DHCP Server 1	192.168.1.100	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Relay Agent Information	<input checked="" type="checkbox"/> Option 82	
Information	<input type="checkbox"/> GS-4012F	

Apply Cancel

33.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application > DHCP** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.



You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See [Section 7.6 on page 83](#) for information on how to do this.

Figure 150 IP Application > DHCP > VLAN

VLAN Setting Status

VID:

DHCP Status: ☒ Server ☐ Relay

Server

Client IP Pool Starting Address:

Size of Client IP Pool:

IP Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

Relay

Remote DHCP Server 1:

Remote DHCP Server 2:

Remote DHCP Server 3:

Relay Agent Information: ☐ Option 82

Information:

Add Cancel Clear

VID	Type	DHCP Status	Delete
2	Server	192.168.2.100/66	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

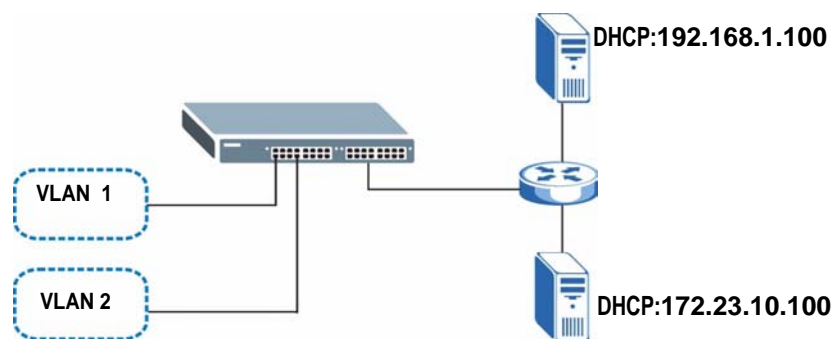
Table 104 IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select whether the Switch should function as a DHCP Server or Relay for the specified VID. If you select Server then fields related to DHCP relay configuration are grayed out and vice versa.
Server	Use this section if you want to configure the Switch to function as a DHCP server for this VLAN.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool. The Switch can issue from 1 to 253 IP addresses to DHCP clients.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the Option 82 check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays Server or Relay for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the Delete check boxes.

33.5.1 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.23.10.100.

Figure 151 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 152 DHCP Relay for Two VLANs Configuration Example

VLAN Setting

Status

VID	2
DHCP Status	<input type="radio"/> Server <input checked="" type="radio"/> Relay
Server	
Client IP Pool Starting Address	0.0.0.0
Size of Client IP Pool	
IP Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Relay	
Remote DHCP Server 1	172.23.10.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	<input type="checkbox"/> Option 82 <input type="checkbox"/> GS-4012F

Add Cancel Clear

VID	Type	DHCP Status	Delete
1	Relay	192.168.1.100	<input type="checkbox"/>

Delete Cancel

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the Switch.

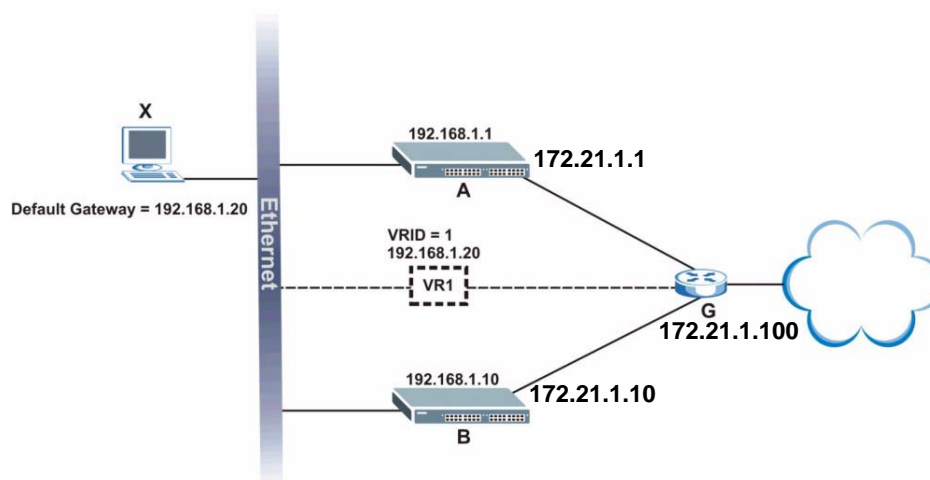
34.1 VRRP Overview

Each host on a network is configured to send packets to a statically configured default gateway (this Switch). The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.20) as the default gateway. If switch **A** has a higher priority, it is the master router. Switch **B**, having a lower priority, is the backup router.

Figure 153 VRRP: Example 1



If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

34.2 VRRP Status

Click **IP Application**, **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

Figure 154 VRRP Status

Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.1/24	1	Master	Alive

Poll Interval(s)

The following table describes the labels in this screen.

Table 105 VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is Master indicating that this Switch functions as the master router. This field is Backup indicating that this Switch functions as a backup router. This field displays Init when this Switch is initiating the VRRP protocol or when the Uplink Status field displays Dead .
Uplink Status	This field displays the status of the link between this Switch and the uplink gateway. This field is Alive indicating that the link between this Switch and the uplink gateway is up. Otherwise, this field is Dead . This field displays Probe when this Switch is check for the link state.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt system statistic polling.

34.3 VRRP Configuration

The following sections describe the different parts of the VRRP Configuration screen.

34.3.1 IP Interface Setup

Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the [Section 7.6 on page 83](#) for more information).

Click **IP Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.



You can only configure VRRP on interfaces with unique VLAN IDs.



Routing domains with the same VLAN ID are not displayed in the table indicated.

Figure 155 VRRP Configuration: IP Interface

Index	Network	Authentication	Key
1	192.168.1.10/24	None	

Apply Cancel

Active ☐

Name

Network

Virtual Router ID

Advertisement Interval

Preempt Mode ☒

Priority

Uplink Gateway

Primary Virtual IP

Secondary Virtual IP

Add Cancel Clear

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 106 VRRP Configuration: IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select None to disable authentication. This is the default setting. Select Simple to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select Simple in the Authentication field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes made in this table.

34.3.2 VRRP Parameters

This section describes the VRRP parameters.

34.3.2.1 Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.



All routers participating in the virtual router must use the same advertisement interval.

34.3.2.2 Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

34.3.2.3 Preempt Mode

If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

34.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

Figure 156 VRRP Configuration: VRRP Parameters

Active	<input type="checkbox"/>
Name	name
Network	192.168.1.10/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	0.0.0.0
Primary Virtual IP	0.0.0.0
Secondary Virtual IP	0.0.0.0

Add Cancel Clear

The following table describes the labels in this screen.

Table 107 VRRP Configuration: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions.
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The Switch checks the link to the uplink gateway.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter 0.0.0.0 .
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes made in this table.
Clear	Click Clear to set the above fields back to the factory defaults.

34.4 VRRP Configuration Summary

To view a summary of all VRRP configurations on the Switch, scroll down to the bottom of the **VRRP Configuration** screen.

Figure 157 VRRP Configuration: Summary

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 108 VRRP Configuring: VRRP Parameters

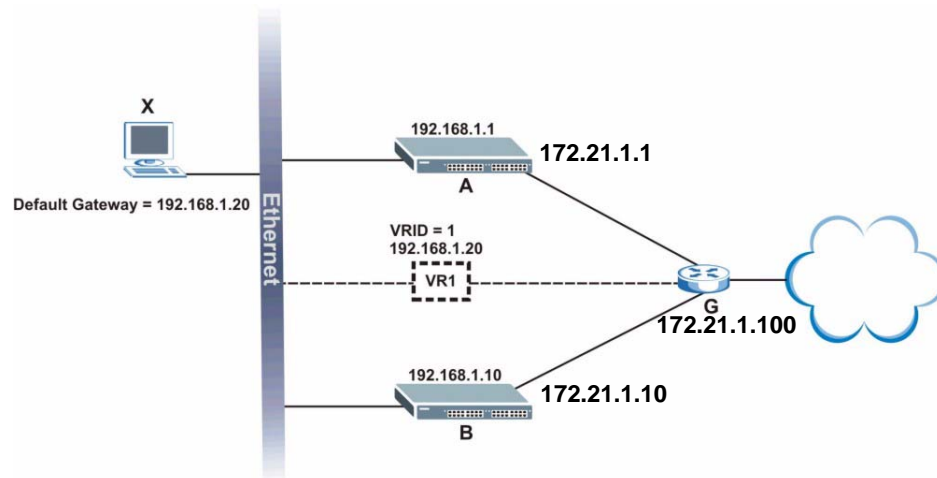
LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled (Yes) or disabled (No).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

34.5 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the Switch.

34.5.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.21.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 158 VRRP Configuration Example: One Virtual Router Network

You want to set switch **A** as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the switches as shown in the figures below.

Figure 159 VRRP Example 1: VRRP Parameter Settings on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example1
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

Figure 160 VRRP Example 1: VRRP Parameter Settings on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example1
Network	192.168.1.10/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 161 VRRP Example 1: VRRP Status on Switch A

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	1	Master	Alive

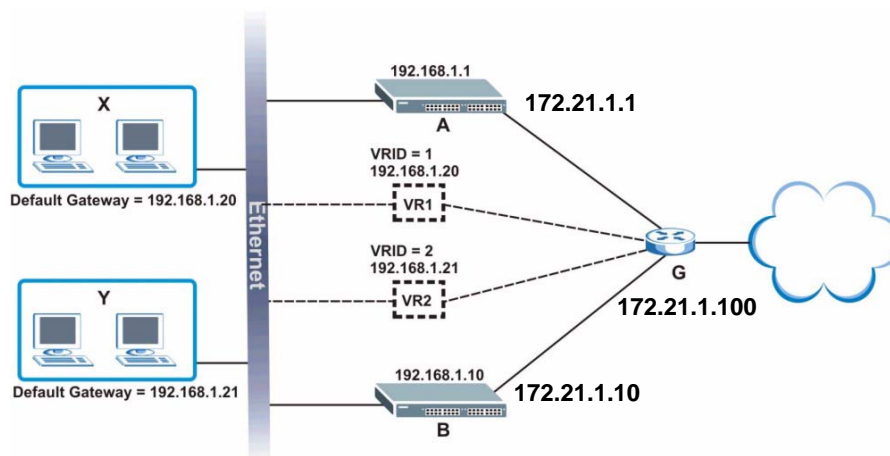
Figure 162 VRRP Example 1: VRRP Status on Switch B

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	1	Backup	Alive

34.5.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch **A** as the master router for virtual router **VR1** and as a backup for virtual router **VR2**. On the other hand, switch **B** is the master for **VR2** and a backup for **VR1**.

Figure 163 VRRP Configuration Example: Two Virtual Router Network

Keeping the VRRP configuration in example 1 for virtual router **VR1** (refer to [Section 34.5.2 on page 274](#)), you need to configure the **VRRP Configuration** screen for virtual router **VR2** on each switch. Configure the VRRP parameters on the switches as shown in the figures below.

Figure 164 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example2
Network	192.168.1.1/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

Figure 165 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example2
Network	192.168.1.10/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

Figure 166 VRRP Example 2: VRRP Status on Switch A

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	2	Backup	Alive
2	Yes	192.168.1.1/24	1	Master	Alive

Figure 167 VRRP Example 2: VRRP Status on Switch B

VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	2	Master	Alive
2	Yes	192.168.1.10/24	1	Backup	Alive

PART V

Management, CLI, Troubleshooting

Maintenance (279)
Access Control (285)
Diagnostic (303)
Syslog (305)
Cluster Management (309)
MAC Table (315)
IP Table (317)
ARP Table (319)
Routing Table (321)
Configure Clone (323)
Introducing Commands (325)
User and Enable Mode Commands (377)
Configuration Mode Commands (383)
Interface Commands (395)
IEEE 802.1Q Tagged VLAN Commands (403)
Multicast VLAN Registration Commands (411)
Routing Domain Command Examples (413)
Troubleshooting (415)

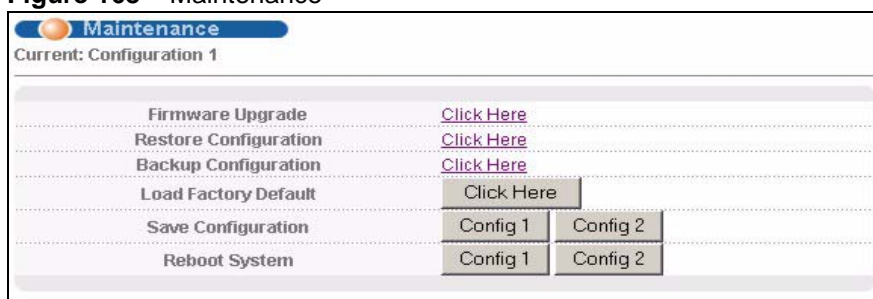
Maintenance

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

35.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management**, **Maintenance** in the navigation panel to open the following screen.

Figure 168 Maintenance



The following table describes the labels in this screen.

Table 109 Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the Switch.
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Load Factory Default	Click Click Here to reset the configuration to the factory default settings.

Table 109 Maintenance (continued)

LABEL	DESCRIPTION
Save Configuration	Click Config 1 to save the current configuration settings to Configuration 1 on the Switch. Click Config 2 to save the current configuration settings to Configuration 2 on the Switch.
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the Switch. Click Config 2 to reboot the system and load Configuration 2 on the Switch. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the Switch.

35.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.
- 2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 169 Load Factory Default: Start

- 3 In the web configurator, click the **Save** button to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

35.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.



Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

35.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 170 Reboot System: Confirmation



- 2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

35.5 Firmware Upgrade

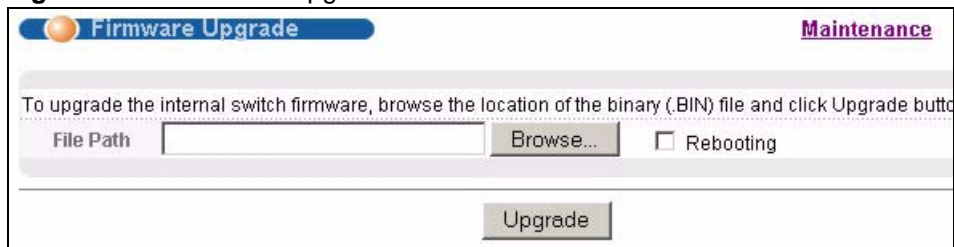
Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 171 Firmware Upgrade



Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** checkbox if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

35.6 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 172 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

35.7 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 173 Backup Configuration

Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Click **Backup**.
- 2 Click **Save** to display the **Save As** screen.
- 3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

35.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

35.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 110 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config		This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

35.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

35.8.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter `open`, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").

- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (`firmware.bin`) to the Switch and renames it to “`ras`”. Similarly, `put config.cfg config` transfers the configuration file on your computer (`config.cfg`) to the Switch and renames it to “`config`”. Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to “`config.cfg`”. See [Table 110 on page 283](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

35.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

35.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the Telnet session immediately.

Access Control

This chapter describes how to control access to the Switch.

36.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 111 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See [Section 45.12.2 on page 334](#) for more information on disabling multi-login.

36.2 The Access Control Main Screen

Click **Management, Access Control** in the navigation panel to display the main screen as shown.

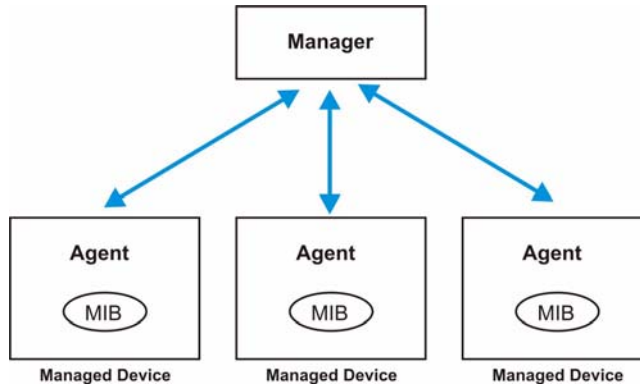
Figure 174 Access Control



36.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 175 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the Switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 112 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

36.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

36.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

36.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with “**1.3.6.1.4.1.890.1.5.8**” is defined in private MIBs. Otherwise, it is a standard MIB OID.

Table 113 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	FanSpeedEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the fan speed returns to the normal operating range.

Table 113 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
temperature	TemperatureEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	GS-4012F: 1.3.6.1.4.1.890.1.5.1.1.2 GS-4024: 1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	RTCNotUpdatedEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the Switch gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when loopguard shuts down a port.

Table 114 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when the Ethernet link is down.
autonegotiation	AutonegotiationFailedEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.

Table 115 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the RADIUS server can be reached.

Table 115 AAA Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
accounting	RADIUSAccountingNotReachableEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAccountingNotReachableEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 116 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 117 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.43.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.43.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.107.7 0.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.107.7 0.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.43.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.43.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.107.7 0.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.107.7 0.2	This trap is sent when the MSTP root switch changes.
mactable	MacTableFullEventOn	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.1 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	GS-4012F: 1.3.6.1.4.1.890.1.5.8.20.37.2.2 GS-4024: 1.3.6.1.4.1.890.1.5.8.13.37.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.

36.3.4 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen. Use this screen to configure your SNMP settings.

Figure 176 Access Control: SNMP

SNMP Access Control Trap Group

General Setting

Version	v2c
Get Community	public
Set Community	public
Trap Community	public

Trap Destination

Version	IP	Port	Username
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	

User Information

Index	Username	Security Level	Authentication	Privacy
1	admin	noauth	MD5	DES

Apply Cancel

The following table describes the labels in this screen.

Table 118 Access Control: SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	<p>Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c).</p> <p>Note: SNMP version 2c is backwards compatible with SNMP version 1.</p>
Get Community	<p>Enter the Get Community string, which is the password for the incoming Get- and GetNext- requests from the management station.</p> <p>The Get Community string is only used by SNMP managers using SNMP version 2c or lower.</p>
Set Community	<p>Enter the Set Community, which is the password for incoming Set- requests from the management station.</p> <p>The Set Community string is only used by SNMP managers using SNMP version 2c or lower.</p>
Trap Community	<p>Enter the Trap Community string, which is the password sent with each trap to the SNMP manager.</p> <p>The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.</p>
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.

Table 118 Access Control: SNMP (continued)

LABEL	DESCRIPTION
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in Management > Access Control > Logins screen).
User Information	Use this section to configure users for authentication with managers using SNMP v3. Note: Use the username and password of the login accounts you specify in this section to create accounts on the SNMP v3 manager.
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: <ul style="list-style-type: none"> • noauth -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • auth - to implement an authentication algorithm for SNMP messages sent by this user. • priv - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 177 Access Control: SNMP: Trap Group

The following table describes the labels in this screen.

Table 119 Access Control: SNMP: Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the SNMP Setting screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See Section 36.3.3 on page 287 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3.6 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.



It is highly recommended that you change the default administrator password (1234).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Access Control** from the navigation panel and then click **Logins** from this screen.

Figure 178 Access Control: Logins

Logins Access Control

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

The following table describes the labels in this screen.

Table 120 Access Control: Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see Chapter 45 on page 325 .
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.4 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

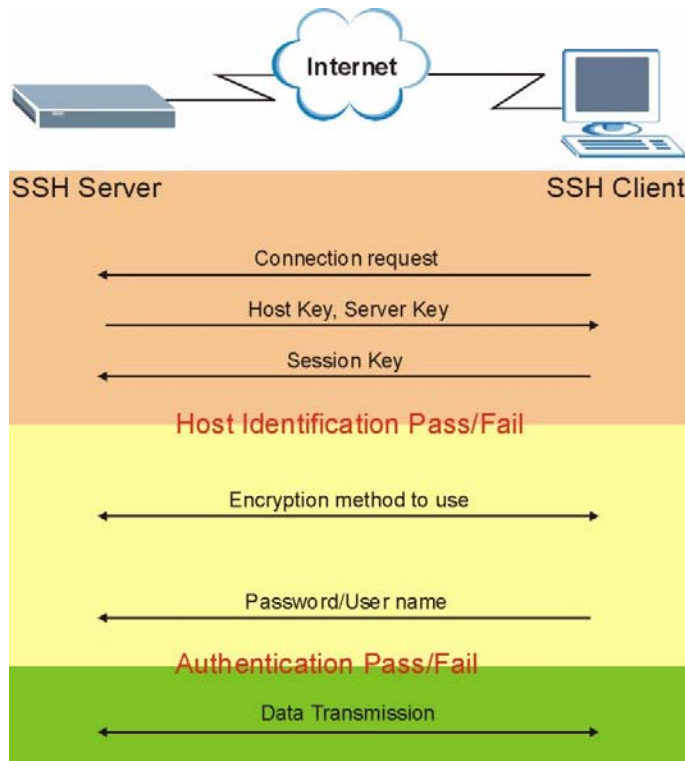
Figure 179 SSH Communication Example



36.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 180 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

36.6 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

36.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

36.7 Introduction to HTTPS

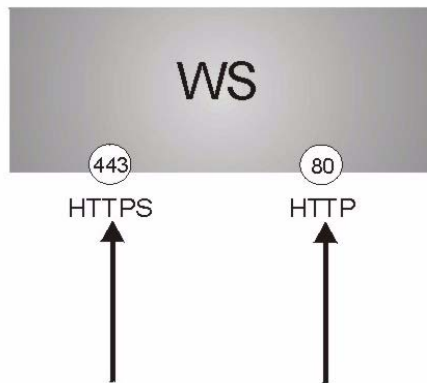
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Switch.

Please refer to the following figure.

- 1** HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).
- 2** HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 181 HTTPS Implementation

If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

36.8 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

36.8.1 Internet Explorer Warning Messages

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 182 Security Alert Dialog Box (Internet Explorer)

36.8.2 Netscape Navigator Warning Messages

When you attempt to access the Switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Switch's certificate into the SSL client.

Figure 183 Security Certificate 1 (Netscape)

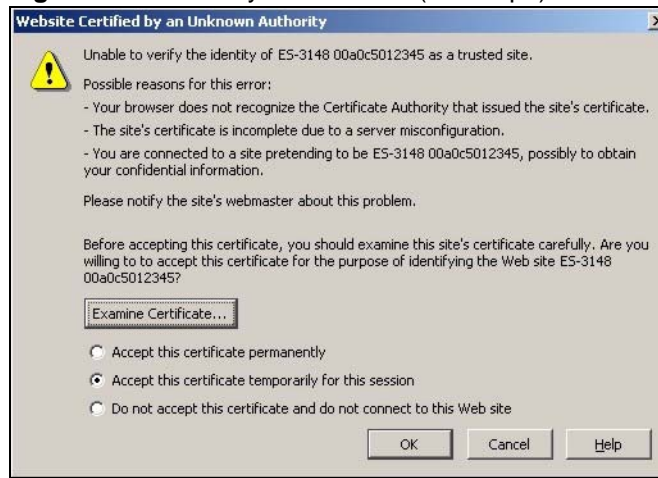
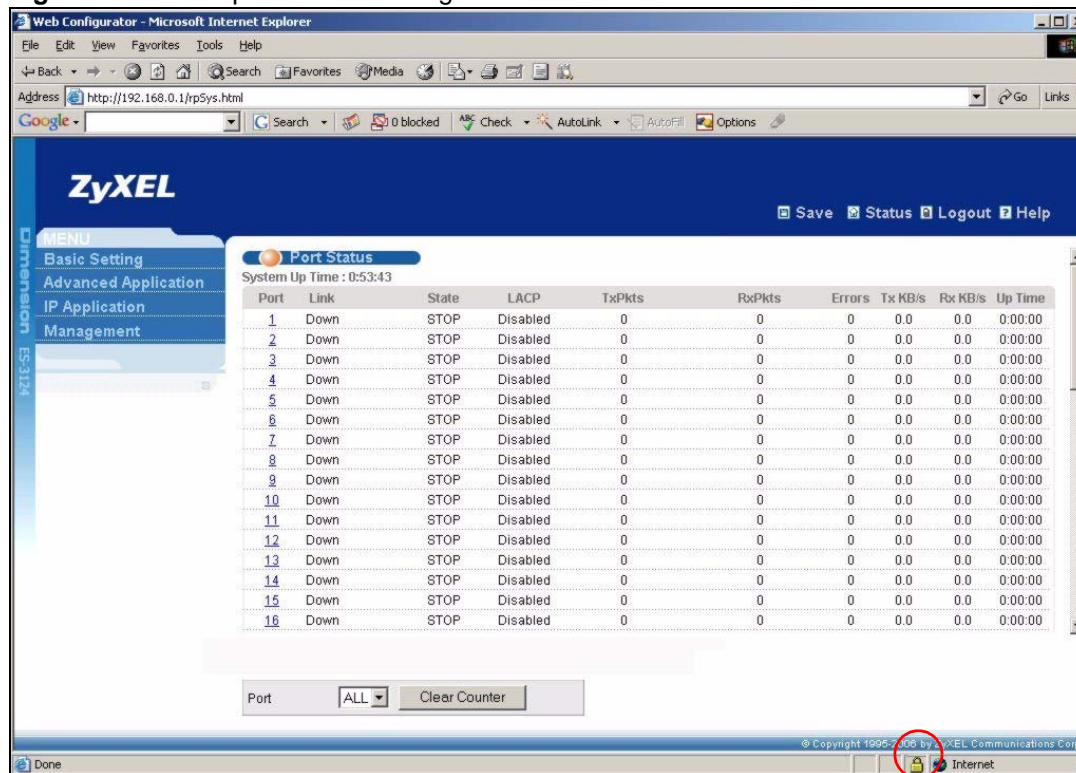


Figure 184 Security Certificate 2 (Netscape)



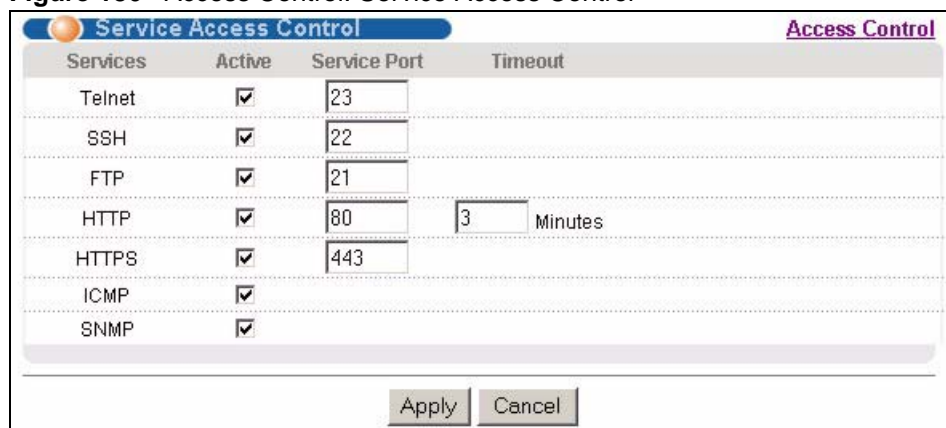
36.8.3 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 185 Example: Lock Denoting a Secure Connection

36.9 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 186 Access Control: Service Access Control

The following table describes the fields in this screen.

Table 121 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Server Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.10 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 187 Access Control: Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 122 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.

Table 122 Access Control: Remote Management (continued)

LABEL	DESCRIPTION
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Diagnostic

This chapter explains the **Diagnostic** screen.

37.1 Diagnostic

Click **Management**, **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 188 Diagnostic

The screenshot shows the 'Diagnostic' screen with a title bar containing a globe icon and the word 'Diagnostic'. Below the title bar is a multi-line text box displaying the results of a ping test:

```
Resolving 192.168.1.23 ... 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Ping Host Successful
```

Below the text box are three sections of controls:

- System Log:** Includes 'Display' and 'Clear' buttons.
- IP Ping:** Includes an 'IP Address' input field and a 'Ping' button.
- Ethernet Port Test:** Includes a 'Port' input field (containing the number '1') and a 'Port Test' button.

The following table describes the labels in this screen.

Table 123 Diagnostic

LABEL	DESCRIPTION
System Log	Click Display to display a log of events in the multi-line text box. Click Clear to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click Port Test to perform an internal loopback test.

Syslog

This chapter explains the syslog screens.

38.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 124 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

38.2 Syslog Setup

Click **Management** and then **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 189 Syslog

Logging type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 0
Interface	<input checked="" type="checkbox"/>	local use 0
Switch	<input checked="" type="checkbox"/>	local use 0
AAA	<input checked="" type="checkbox"/>	local use 0
IP	<input checked="" type="checkbox"/>	local use 0

The following table describes the labels in this screen.

Table 125 Syslog

LABEL	DESCRIPTION
Syslog	Select Active to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

38.3 Syslog Server Setup

Click **Management** and then **Syslog** in the navigation panel to display the **Syslog Setup** screen. Click the **Syslog Server Setup** link to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 190 Syslog: Server Setup

The screenshot shows the 'Syslog Server Setup' configuration interface. At the top, there's a title bar with 'Syslog Server Setup' and a link 'Syslog Setup'. Below this is a form with three main sections: 'Active' with a checkbox, 'Server Address' with a text input field containing '0.0.0.0', and 'Log Level' with a dropdown menu set to 'Level 0'. Underneath the form are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the page, there is a table with five columns: 'Index', 'Active', 'IP Address', 'Log Level', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 126 Syslog: Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's Delete check box and click Delete to remove the entry.
Cancel	Click Cancel to begin configuring this screen afresh.

Cluster Management

This chapter introduces cluster management.

39.1 Cluster Management Status Overview

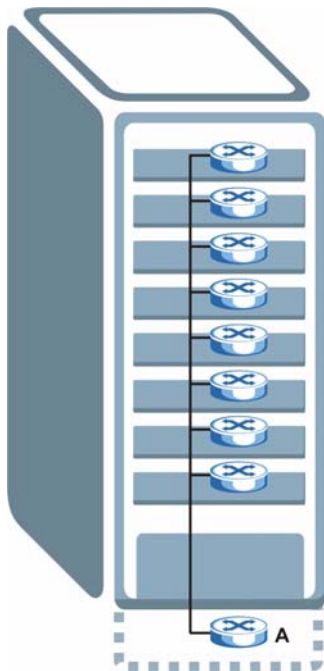
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 127 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 191 Clustering Application Example



39.2 Cluster Management Status

Click **Management**, **Cluster Management** in the navigation panel to display the following screen.



A cluster can only have one manager.

Figure 192 Cluster Management: Status

Clustering Management Status

Configuration

Status

Manager

Manager

00:13:49:00:00:02

The Number Of Member = 1

Index	MacAddr	Name	Model	Status
1	00:a0:c5:01:23:46		GS-2024	Online

The following table describes the labels in this screen.

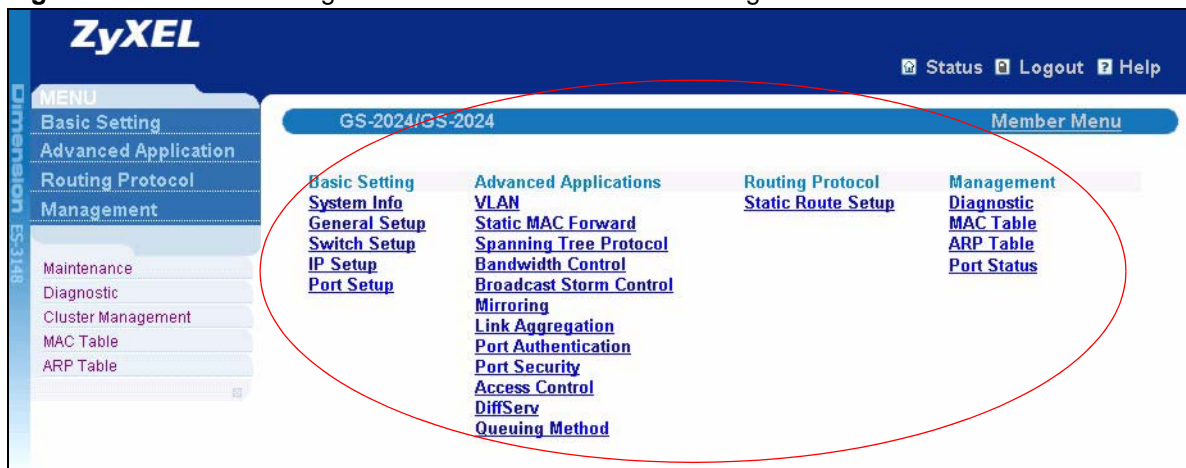
Table 128 Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 193 on page 311).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

39.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 193 Cluster Management: Cluster Member Web Configurator Screen



39.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 194 Example: Uploading Firmware to a Cluster Member Switch

```

C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner   group           3042210 Jul  01 12:00 ras
-rw-rw-rw-  1 owner   group           393216 Jul  01 12:00 config
--w--w--w-  1 owner   group              0 Jul  01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-  1 owner   group              0 Jul  01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 3701t0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>

```

The following table explains some of the FTP parameters.

Table 129 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
3601t0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

39.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 195 Clustering Management Configuration

Clustering Management Configuration

[Status](#)

Clustering Manager:

Active
☒

Name
Master

VID
1

Apply

Cancel

Clustering Candidate:

List
00:a0:c5:01:23:46/GS-2024/

Password

Add

Cancel

Refresh


Index	MacAddr	Name	Model	Remove
<div> <div>Remove</div> <div>Cancel</div> </div>				

The following table describes the labels in this screen.

Table 130 Clustering Management Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.

Table 130 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the Remove button to remove a cluster member switch from the cluster.
Cancel	Click Cancel to begin configuring this screen afresh.

MAC Table

This chapter introduces the **MAC Table** screen.

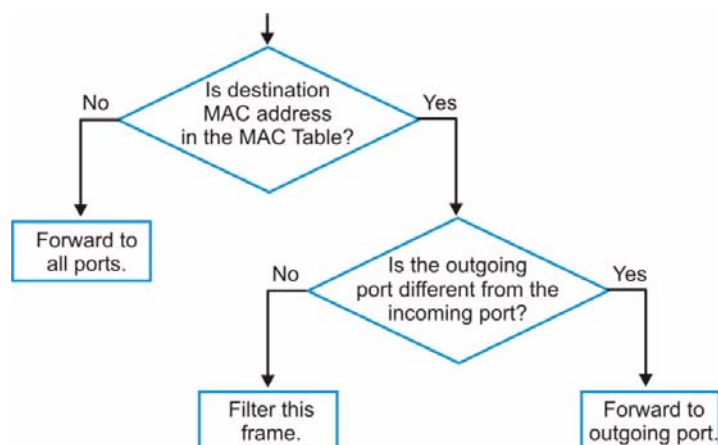
40.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the MAC table to determine how to forward frames. See the following figure.

- 1 The Switch examines a received frame and learns the port on which this source MAC address came.
 - 2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
- If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 196 MAC Table Flowchart



40.2 Viewing the MAC Table

Click **Management, MAC Table** in the navigation panel to display the following screen.

Figure 197 MAC Table



MAC Table					
Sort by					
<input type="button" value="MAC"/> <input type="button" value="VID"/> <input type="button" value="Port"/>					
Index	MAC Address	VID	Port	Type	
1	00:85:a0:01:01:00	1	8	dynamic	
2	00:85:a0:01:01:04	1	8	dynamic	
3	00:a0:c5:00:00:01	1	2	dynamic	
4	00:a0:c5:fe:ea:71	1	CPU	static	
5	00:a0:c5:fe:ea:71	2	CPU	static	

The following table describes the labels in this screen.

Table 131 MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the Static MAC Forwarding screen).

IP Table

This chapter introduces the IP table.

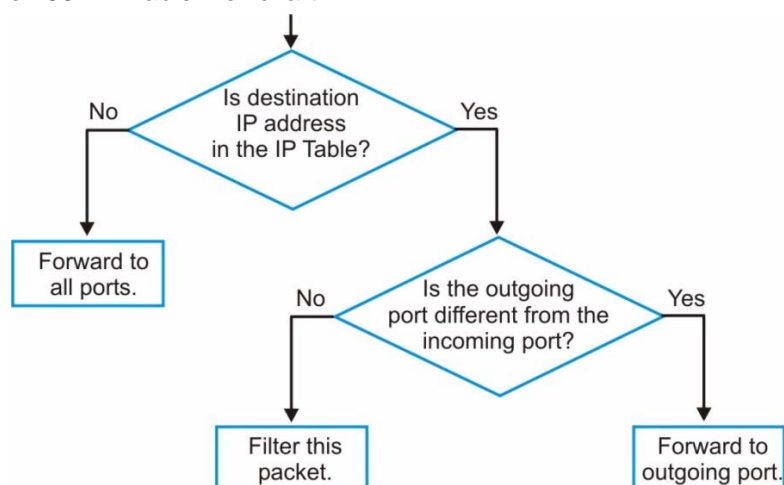
41.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. It shows what device IP address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

The Switch uses the IP table to determine how to forward packets. See the following figure.

- 1 The Switch examines a received packet and learns the port on which this source IP address came.
- 2 The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the IP table.
 - If the Switch has already learned the port for this IP address, then it forwards the packet to that port.
 - If the Switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion.
 - If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

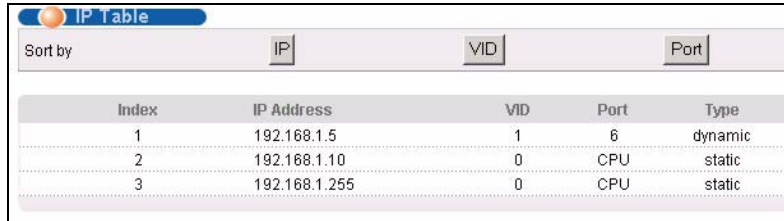
Figure 198 IP Table Flowchart



41.2 Viewing the IP Table

Click **Management, IP Table** in the navigation panel to display the following screen.

Figure 199 IP Table



Index	IP Address	VID	Port	Type
1	192.168.1.5	1	6	dynamic
2	192.168.1.10	0	CPU	static
3	192.168.1.255	0	CPU	static

The following table describes the labels in this screen.

Table 132 IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays CPU to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

ARP Table

This chapter introduces ARP Table.

42.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

42.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

42.2 Viewing the ARP Table

Click **Management, ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 200 ARP Table

ARP Table			
Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

The following table describes the labels in this screen.

Table 133 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the Static MAC Forwarding screen).

Routing Table

This chapter introduces the routing table.

43.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach. The Switch automatically updates the routing table with the RIP information received from other Ethernet devices.

43.2 Viewing the Routing Table

Use this screen to view routing table information. Click **Management, Routing Table** in the navigation panel to display the screen as shown.

Figure 201 Routing Table Status

Routing Table Status					
Index	Destination	Gateway	Interface	Metric	Type
1	192.168.1.0/24	192.168.1.1	192.168.1.1	1	STATIC
2	10.10.10.0/24	10.10.10.1	10.10.10.1	1	STATIC

The following table describes the labels in this screen.

Table 134 Routing Table Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route; OSPF - added as an OSPF interface, RIP - learned from incoming RIP packets or STATIC - added as a static entry.

Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

44.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management, Configure Clone** to open the following screen.

Figure 202 Configure Clone

Configure Clone

Source Destination

Port

Port Features

Basic Setting

- ☐ Active
- ☐ Name
- ☐ Speed / Duplex
- ☐ BPDU Control
- ☐ Flow Control
- ☐ Intrusion Lock

Advanced Application

- ☐ VLAN1q
- ☐ VLAN1q Member
- ☐ Bandwidth Control
- ☐ VLAN Stacking
- ☐ Port Security
- ☐ Broadcast Storm Control
- ☐ Mirroring
- ☐ Port Authentication
- ☐ Queuing Method
- ☐ IGMP Filtering
- ☐ Spanning Tree Protocol
- ☐ Multiple Rapid Spanning Tree Protocol
- ☐ Port-based VLAN
- ☐ MAC Authentication
- ☐ Two-rate three color marker
- ☐ Ethernet OAM
- ☐ Loop Guard
- ☐ ARP Inspection
- ☐ DHCP Snooping

Apply Cancel

The following table describes the labels in this screen.

Table 135 Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the Source label. This port's attributes are copied. Enter the destination port or ports under the Destination label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: <ul style="list-style-type: none">• 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports.• 2-6 indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the Basic Setting menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the Advanced Application menus) should be copied to the destination ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Introducing Commands

This chapter introduces commands and gives a summary of commands available.

45.1 Overview

In addition to the web configurator, you can use commands to configure the Switch. Use commands for advanced Switch diagnosis and troubleshooting. If you have problems with your Switch, customer support may request that you issue some of these commands to assist them in troubleshooting.



See the web configurator parts of this User's Guide for background information on features configurable by the web configurator.

45.2 Accessing the CLI

You can use a direct console connection or Telnet to access the command interpreter on the Switch.



The Switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

- By default, multiple command interpreter management session are allowed via either the console port or Telnet. However, no more than nine concurrent login sessions are allowed.
- Use the `configure multi-login` command in the configuration mode to limit concurrent logins to one. Console port access has higher priority.

45.2.1 The Console Port

Connect to the Switch's console port using a terminal emulation software configured to the following settings:

- VT100 terminal emulation

- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control

45.2.1.1 Initial Screen

When you turn on your Switch, it performs several internal tests as well as line initialization. You can view the initialization information using the console port. After the initialization, the login screen displays (refer to [Section 45.3 on page 326](#)).

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:13:49:00:00:01
initialize switch, ethernet address: 00:13:49:00:00:02
Initializing switch unit 0...
Initializing MSTP.....
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Press ENTER to continue...
```

Use the following steps to telnet into your Switch.

- 1 For local management, connect your computer to the RJ-45 management port (labeled **MGMT**) on the Switch.
- 2 Make sure your computer IP address and the Switch IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type `telnet 192.168.0.1` (the default management IP address) and click **OK**.
- 3 A login screen displays (refer to [Section 45.3 on page 326](#)).

45.3 The Login Screen

After you have successfully established a connection to the Switch using a direct console connection or Telnet, a login screen displays as shown below. For your first login, enter the default administrator login username “admin” and password “1234”.

```
Enter User Name : admin
Enter Password : XXXX
```

45.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in `courier new` font.

- The required fields in a command are enclosed in angle brackets `<>`, for instance, `ping <ip>` means that you must specify an IP number for this command.
- The optional fields in a command are enclosed in square brackets `[]`, for instance, `configure snmp-server [contact <system contact>] [location <system location>]` means that the contact and location fields are optional.
- “Command” refers to a command used in the command line interface (CLI command).
- The `|` symbol means “or”.
- The entry `<cr>` in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up or down arrow key to scroll through the command history list.
- You may enter a unique part of a command and press [TAB] to have the Switch automatically display the full command. For example, if you enter “`config`” and press [TAB], the full command of “`configure`” automatically displays.
- Each interface refers to an Ethernet port on the Switch. Commands configured after the interface command correspond to those ports.
- Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

45.5 Changing the Password

This command is used to change the password for Enable mode. By default the same password is used to enter the command line interface (CLI) and Enable and Config modes of the CLI.

The password you change with this command is required to enter Enable and Config modes of the CLI.

Syntax:

```
password <password>
```

where

<code>password <password></code>	=	Specifies the new password (up to 32 alphanumeric characters) users have to type in to enter Enable and Config modes.
--	---	---

45.6 Creating a New IP Interface

Use the `ip address` command to create a new IP interface (one suitable for your network) for VLAN 1. After you create a new IP interface you can use this IP address for Switch management. The following example shows you how to create an IP interface for the IP address 172.23.0.1 with the subnet mask 255.255.255.0:

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ip address 172.23.0.1 255.255.255.0
```

45.7 Privilege Levels

You can use a command whose privilege level is equal to or less than that of your login account. For example, if your login account has a privilege level of 12, you can use all commands with privilege levels from 0 to 12. 0 privilege level commands are available to all login accounts.



If you use an external RADIUS server to authenticate users, you can use a VSA (Vendor Specific Attribute) to configure a privilege level for an account on the RADIUS server. See [Section 23.2.4 on page 193](#) for more information.

Use the following commands to specify privilege levels for login accounts.

Syntax:

```
logins username <username> password <password>
logins username <username> privilege <0-14>
```

where

username <username>	=	Specifies a new user (up to 32 alphanumeric characters). Enter a user name to change the settings of an existing account.
password <password>	=	Specifies the new password (up to 32 alphanumeric characters) for this user.
privilege <0-14>	=	Assigns a privilege level for the user.

45.8 Command Modes

There are three command modes: **User**, **Enable** and **Configure**. The modes (and commands) available to you depend on what level of privilege your account has. See [Section 45.7 on page 328](#) for more information on setting up privilege levels.

When you first log into the command interpreter with a read-only account (having a privilege of 0), the initial mode is the User mode. The User mode commands are a subset of Enable mode commands. The User mode command prompt ends with an angle bracket (>).

To enter Enable mode, type `enable` and enter the administrator password when prompted (the default is 1234). When you enter Enable mode, the command prompt changes to the pound sign (#). If you log into the command interpreter as an administrator you automatically enter Enable mode.

The following table describes command interpreter modes and how to access them.

Table 136 Command Interpreter Mode Summary

MODE	DESCRIPTION	HOW TO LOGIN/ACCESS	PROMPT
User	Commands available in this mode are a subset of enable mode. You can perform basic tests and display general system information.	Default login level for a read-only account.	<code>sysname></code> The first part of the prompt is the system name. In the CLI examples in this User's Guide, the system name is always "sysname".
Enable	Commands available in this mode allow you to save configuration settings, reset configuration settings as well as display further system information. This mode also contains the <code>configure</code> command which takes you to config mode.	Default login level for accounts with a privilege of 13 or 14. Read-only accounts (with a privilege of 0-12) need to type the <code>enable</code> command and enter enable mode password.	<code>sysname#</code>
Config	Commands available in this mode allow you to configure settings that affect the Switch globally.	Type <code>config</code> in enable mode.	<code>sysname(config)#</code>
Command modes that follow are sub-modes of the config mode and can only be accessed from within the config mode.			
Config-vlan	This is a sub-mode of the config mode and allows you to configure VLAN settings.	Type <code>vlan</code> followed by a number (between 1 to 4094). For example, <code>vlan 10</code> to configure settings for VLAN 10.	<code>sysname(config-vlan)#</code>
Config-interface	This is a sub-mode of the config mode and allows you to configure port related settings.	Type <code>interface port-channel</code> followed by a port number. For example, <code>interface port-channel 8</code> to configure port 8 on the Switch.	<code>sysname(config-interface)#</code>
Config-mvr	This is a sub-mode of the config mode and allows you to configure multicast VLAN settings.	To enter MVR mode, enter <code>mvr</code> followed by a VLAN ID (between 1 and 4094). For example, enter <code>mvr 2</code> to configure multicast settings on VLAN 2.	<code>sysname(config-mvr)#</code>

Enter `exit` to quit from the current mode or enter `logout` to exit the command interpreter.

45.9 Getting Help

The system includes a help facility to provide you with the following information about the commands:

- List of available commands under a command group.
- Detailed descriptions of the commands.

45.9.1 List of Available Commands

Enter “help” to display a list of available commands and the corresponding sub commands.

```
sysname> help
  Commands available:

  help
  logout
  exit
  history
  enable
  show ip <cr>
  show hardware-monitor <C|F>
  show system-information
  show alarm-status
  show cpu-utilization
  show version flash
  show version <cr>
  ping <ip|host-name> <cr>
  ping <ip|host-name> [vlan <vlan-id>][...]
  ping help
  traceroute <ip|host-name> <cr>
  traceroute <ip|host-name> [vlan <vlan-id>][...]
  traceroute help
  ssh <l|2> <[user@]dest-ip> <cr>
  ssh <l|2> <[user@]dest-ip> [command </>]
sysname>
```

Enter “?” to display a list of commands you can use.

```
sysname> ?
  enable          Turn on privileged commands
  exit            Exit from the EXEC
  help            Description of the interactive help system
  history          Show a list of previously run commands
  logout          Exit from the EXEC
  ping            Exec ping
  show            Show system information
  ssh             SSH client
  traceroute      Exec traceroute
sysname>
```

Enter `<command> help` to display detailed sub commands and parameters.

```
sysname> ping help
  Commands available:

  ping <ip|host-name>
    <
      [ in-band|out-of-band|vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
sysname>
```

Enter `<command> ?` to display detailed help information about the sub commands and parameters.

```
sysname> ping ?
  <ip|host-name>      destination ip address
  help                Description of ping help

sysname>
```

45.10 Using Command History

The Switch keeps a list of recently used commands available to you for reuse. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

```
sysname> history
  enable
  exit
  show ip
  history
sysname>
```

45.11 Saving Your Configuration

After you set the Switch settings with the configuration commands, use the `write memory` command to save the changes permanently.



The `write memory` command is not available in User mode.



You must save your changes after each CLI session. All unsaved configuration changes are lost once you restart the Switch.

```
sysname# write memory
```

45.11.1 Switch Configuration File

When you configure the Switch using either the CLI (Command Line Interface) or web configurator, the settings are saved as a series of commands in a configuration file on the Switch. You can perform the following with a configuration file:

- Back up Switch configuration once the Switch is set up to work in your network.
- Restore Switch configuration.
- Use the same configuration file to set all switches (of the same model) in your network to the same settings.



You may also edit a configuration file using a text editor.



Make sure you use valid commands. The Switch rejects configuration files with invalid or incomplete commands.

45.11.2 Logging Out

In User or Enable mode, enter the `exit` or `logout` command to log out of the CLI. In Config mode entering `exit` takes you out of the Config mode and into Enable mode and entering `logout` logs you out of the CLI.

45.12 Command Summary

The following sections summarize the commands available in the Switch together with a brief description of each command. Commands listed in the tables are in the same order as they are displayed in the CLI. See the related section in the User's Guide for more background information.

45.12.1 User Mode

The following table describes the commands available for User mode.

Table 137 Command Summary: User Mode

COMMAND		DESCRIPTION	PRIVILEGE
help		Displays help information.	0
logout		Exits from the CLI.	0
exit		Logs out from the CLI.	0
history		Displays a list of previously command(s) that you have executed. The Switch stores up to 256 commands in history.	0
enable		Accesses Enable (or privileged) mode. See Section 45.12.2 on page 334 . Enable the highest privilege level for executing commands.	0
	<0-14>	Accesses Enable mode commands up to the privilege level specified. See Section 45.12.2 on page 334 .	0
		Accesses Enable (or privileged) mode. See Section 45.12.2 on page 334 .	0
show	ip	Displays IP related information.	0
	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	0
	system-information	Displays general system information.	0
	alarm-status	Display which alarms are enabled on the Switch as well as the LED status of the alarms.	0
	cpu-utilization	Display statistics about the utilization of the CPU on the Switch.	0
	version flash	Display the version of the currently installed firmware on the flash memory.	0
	version <cr>	Display the version of the currently running firmware on the Switch.	0
ping	<IP host-name>	Sends Ping request to an Ethernet device.	0
	<IP host-name> [vlan <vlan-id>] [size <0-1472>] [-t]	Sends Ping request to an Ethernet device in the specified VLAN(s) with the specified parameters.	0
	help	Displays command help information.	0
traceroute	<ip host-name>	Determines the path a packet takes to a device.	0
	<ip host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device in a VLAN.	0
	help	Displays command help information.	0
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.	0

45.12.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 138 Command Summary: Enable Mode

COMMAND			DESCRIPTION	PRIVILEGE
baudrate <1 2 3 4 5>			Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).	13
boot	config <index>		Restarts the system with the specified configuration file.	13
clear	arp inspection	filter	Delete all ARP inspection filters from the Switch.	13
	arp inspection	log	Delete all ARP inspection log entries from the Switch.	13
	arp inspection	statistics	Delete all statistics records of ARP packets going through the Switch.	13
	arp inspection	statistics vlan <vlan-list>	Delete statistics records of ARP packets going through the Switch for the specified VLAN(s).	13
	dhcp snooping database	statistics	Delete all statistics records of DHCP requests going through the Switch.	13
	loopguard		Clears all loopguard counters.	13
configure			Accesses Configuration mode. See Section 45.12.3 on page 343 .	13
copy	running-config tftp <ip> <remote-file>		Backs up running configuration to the specified TFTP server with the specified file name.	13
	running-config interface port- channel <port> <port-list>		Clones (copies) the attributes from the specified port to other ports.	13
	running-config interface port- channel <port> <port-list>	[bandwidth-limit]	Copies the specified attributes from one port to other ports.	13
	tftp	config <index> <ip> <remote- file>	Restores configuration with the specified filename from the specified TFTP server to the specified configuration file on the router.	13
		flash <ip> <remote-file>	Restores firmware via TFTP.	13
disable			Exits Enable (or privileged) mode.	13
enable			Accesses Enable (or privileged) mode. Enables the highest privilege level for executing commands.	0

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	<0-14>		Accesses Enable mode commands up to the privilege level specified.	0
erase	running-config		Resets to the factory default settings.	13
		help	Displays help information for this command.	13
		interface port-channel <port-list> [bandwidth-limit...]	Resets to the factory default settings on a per port basis and optionally on a per feature configuration basis.	13
ethernet oam	remote-loopback test <port>	[<number of packets> [<packet size>]]	Performs a loopback test from the specified port, optionally specifies how many and the size of packets sent in the loopback test.	13
exit			Exits Enable (or privileged) mode.	0
help			Displays help information.	0
history			Displays a list of command(s) that you have previously executed.	0
igmp-flush			Removes all IGMP information.	13
kick	tcp <Session ID>		Disconnects the specified TCP session.	13
logout			Exits Enable (or privileged) mode.	0
mac-flush			Clears the MAC address table.	13
	<port-num>		Removes all learned MAC address on the specified port(s).	13
no	arp		Flushes the ARP table entries.	13
	arp	inspection filter <mac-addr> vlan <vlan-id>	Specify the ARP inspection record you want to delete from the Switch. The ARP inspection record is identified by the MAC address and VLAN ID pair.	13
	interface	<port-number>	Clears all counters on the specified port.	13
	logging		Disables syslog logging.	13
ping <IP host-name>			Sends Ping request to an Ethernet device.	0
	[vlan <vlan-id>][...]		Sends Ping request to an Ethernet device in the specified VLAN(s).	13
reload	config <index>		Restarts the system and use the specified configuration file.	13
renew dhcp snooping database			Loads dynamic bindings from the default DHCP snooping database.	13

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
renew dhcp snooping database	<tftp://host/ filename>		Loads dynamic bindings from the specified DHCP snooping database.	13
show	aaa	authentication	Displays whether authentication and privilege checking is enabled on the Switch and what methods are used for authentication.	3
		authentication enable	Displays the authentication method(s) for checking privilege level of administrators.	3
		authentication login	Displays the authentication methods for administrator login accounts.	3
		accounting	Displays accounting settings configured on the Switch.	3
		accounting commands	Displays accounting settings for recording command events.	3
		accounting dot1x	Displays accounting settings for recording IEEE 802.1x session events.	3
		accounting exec	Displays accounting settings for recording administrative sessions via SSH, Telnet or the console port.	3
		accounting system	Displays accounting settings for recording system events, for example system shut down, start up, accounting enabled or accounting disabled.	3
		accounting update	Display the update period setting on the Switch for accounting sessions.	3
	alarm-status		Displays alarm status and configuration.	0
	arp inspection		Displays ARP inspection configuration details.	3
		filter	Displays the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet.	3
		filter [<mac-addr>] [vlan <vlan-id>]	Displays the current list of MAC address filters based on the MAC address or VLAN ID contained in the filter.	3
		interface port-channel <port-list>	Displays the ARP inspection settings for the specified port(s).	3
		log	Displays the log settings configured on the Switch. It also displays the log entries recorded on the Switch.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		statistics	Displays statistics regarding the total number of ARP packets received on the Switch.	3
		statistics vlan <vlan-list>	Displays statistics regarding the total number of ARP packets received on the Switch based on the VLAN(s) specified.	3
		vlan <vlan-list>	Displays ARP inspection settings for the specified VLAN(s).	3
	classifier		Displays all classifier related information.	3
		[name]	Displays the specified classifier related information.	3
	cluster		Displays cluster management status.	3
		candidates	Displays cluster candidate information.	3
		member	Displays the MAC address of the cluster member(s).	3
		member config	Displays the configuration of the cluster member(s).	3
		member mac <mac-addr>	Displays the status of the cluster member(s).	3
	cpu-utilization		Displays the CPU utilization statistics on the Switch.	0
	dhcp	relay <vlan-id>	Displays DHCP relay settings.	3
		server	Displays DHCP server settings.	3
		server <vlan-id>	Displays DHCP server settings in a specified VLAN.	3
		smart-relay	Displays global DHCP relay settings.	3
		snooping	Displays DHCP snooping configuration on the Switch.	3
		snooping binding	Displays the DHCP binding table.	3
		snooping database	Displays DHCP snooping database update statistics and settings.	3
		snooping database detail	Displays DHCP snooping database update statistics in full detail form.	3
	diffserv		Displays general DiffServ settings.	3
	ethernet oam	discovery <port-list>	Displays OAM configuration details and operational status of the specified ports.	3
	ethernet oam	statistics <port-list>	Displays the number of OAM packets transferred for the specified ports.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	ethernet oam	summary	Displays the configuration details of each OAM activated port.	3
	garp		Displays GARP information.	3
	hardware-monitor	<C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	0
	https		Displays the HTTPS information.	3
		certificate	Displays the HTTPS certificates.	3
		key <rsa dsa>	Displays the HTTPS key.	3
		session	Displays current HTTPS session(s).	3
		timeout	Displays the HTTPS session timeout.	3
	igmp-filtering	profile	Displays IGMP filtering profile settings.	3
	igmp-snooping		Displays global IGMP snooping settings.	3
		vlan	Displays the VLANs on which IGMP snooping is enabled.	3
		querier	Displays the IGMP querier mode settings on each port.	3
	interfaces <port-number>		Displays current interface status.	3
	interfaces config <port-list>		Displays current interface configuration.	3
		bandwidth-control	Displays bandwidth control settings.	3
		bstorm-control	Displays broadcast storm control settings.	3
		egress	Displays outgoing port information.	3
		igmp-filtering	Displays IGMP filtering settings.	3
		igmp-group-limited	Displays the IGMP group limit.	3
		igmp-immediate-leave	Displays the IGMP Immediate Leave setting.	3
		igmp-query-mode	Displays the IGMP query mode for the specified port(s).	3
	ip		Displays IP related information.	0
		arp	Displays the ARP table.	3
		dvmrp group	Displays DVMRP group information.	3
		dvmrp interface	Displays DVMRP interface information.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		dvmrp neighbor	Displays DVMRP neighbor information.	3
		dvmrp prune	Displays the DVMRP prune information.	3
		dvmrp route	Displays the DVMRP routes.	3
		igmp group	Displays multicast group details for each port(s).	3
		igmp interface	Displays IGMP settings for each IP interface.	3
		igmp multicast	Displays details about known and unknown multicast frames passing through the Switch on the specified port(s).	3
		igmp timer	Displays IGMP counter and timer settings for each IP interface.	3
		iptable all [IP VID PORT]	Displays the IP address table. You can sort the table based on the IP address, VLAN ID or the port number.	3
		iptable count	Displays the number of IP interfaces configured on the Switch.	3
		iptable static	Displays the static IP address table.	3
		ospf database	Displays OSPF link state database information.	3
		ospf interface	Displays OSPF interface settings.	3
		ospf neighbor	Displays OSPF neighbor information.	3
		protocol-based-vlan	Displays protocol based VLAN settings on the port(s).	3
		route	Displays IP routing information.	3
		route static	Displays IP static route information.	3
		source binding	Displays the static bindings (IP to MAC address) configured on the Switch.	3
		source binding [<mac-addr>] [...]	Displays the static bindings configured on the Switch based on MAC address or VLAN ID of the static binding.	3
		source binding help	Displays help information for the source binding command.	3
		tcp	Displays IP TCP information.	3
		udp	Displays IP UDP information.	3
	lacp		Displays LACP (Link Aggregation Control Protocol) settings.	3
	logging		Displays system logs.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	logins		Displays login account information.	3
	loopguard		Displays which ports have loopguard enabled as well as their status.	3
	mac	address-table <all [mac vid port]>	Displays MAC address table. You can sort by MAC address, VID or port.	3
		address-table count	Displays the total number of MAC addresses in the MAC address table.	3
		address-table static	Displays the static MAC address table.	3
		address-table vlan <vlan-id>	Displays the static MAC address table for the specified VLAN.	3
		address-table vlan <vlan-id> <sort>	Displays the static MAC address table for the specified VLAN. Sorted by MAC, Port or type.	3
		address-table port <port-list>	Displays the static MAC address table for the specified port(s).	3
		address-table port <port-list> <sort>	Displays the static MAC address table for the specified port(s). Sorted by MAC, Port or type.	3
	mac-aging-time		Displays MAC learning aging time.	3
	mac-authentication		Displays MAC authentication settings for the Switch.	3
	mac-authentication	config	Displays MAC authentication settings on a port by port basis with authentication statistics for each port.	3
	mac-count		Displays the count of MAC addresses learnt.	3
	mrstp <tree-index>		Displays multiple rapid spanning tree configuration for the specified tree.	3
	mstp		Displays MSTP configuration for the Switch.	3
		instance <0-16>	Displays MSTP instance configuration.	3
	multicast		Displays multicast status, including the port number, vlan ID and multicast group number of multicast group members on the Switch.	3
		vlan	Displays multicast VLAN status.	3
	multi-login		Displays multi-login information	3
	mvr		Displays all MVR settings.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		<vlan-id>	Displays the specified MVR group settings.	3
	policy		Displays all policy related information.	3
		[name]	Displays the specified policy related information.	3
	port-access-authenticator		Displays all port authentication settings.	3
		[port-list]	Displays port authentication settings on the specified port(s).	3
	port-security		Displays all port security settings.	3
		[port-list]	Displays port security settings on the specified port(s).	3
	radius-accounting		Displays RADIUS accounting server settings.	3
	radius-server		Displays RADIUS server settings.	3
	remote-management		Displays all secured client information.	3
		[index]	Displays the specified secured client information.	3
	router	dvmrp	Displays DVMRP settings.	3
		igmp	Displays global IGMP settings.	3
		ospf	Displays OSPF settings.	3
		ospf area	Displays OSPF area settings.	3
		ospf network	Displays OSPF network (or interface) settings.	3
		ospf redistribute	Displays OSPF redistribution settings.	3
		ospf virtual-link	Displays OSPF virtual link settings.	3
		rip	Displays global RIP settings.	3
		vrrp	Displays VRRP settings.	3
	running-config		Displays current operating configuration.	3
		interface port-channel <port-list> [bandwidth-limit...]	Displays current operating configuration on a port by port basis. Optionally specifies which settings are displayed.	3
		help	Displays the help information for this command.	3
	service-control		Displays service control settings.	3
	snmp-server		Displays SNMP settings.	3
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.	3
	ssh		Displays general SSH settings.	3

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		known-hosts	Displays known SSH hosts information.	3
		key <rsa1 rsa dsa>	Displays internal SSH public and private key information.	3
		session	Displays current SSH session(s).	3
	subnet-vlan		Displays subnet based VLAN settings on the Switch.	3
	system-information		Displays general system information.	0
	tacacs-server		Displays TACACS+ server settings.	3
	tacacs-accounting		Displays TACACS+ accounting server settings.	3
	time		Displays current system time and date.	3
	timesync		Displays time server information.	3
	trunk		Displays link aggregation information.	3
	version		Displays the firmware version running on the Switch.	0
		flash	Displays the firmware version on the flash memory of the Switch.	0
	vlan		Displays the status of all VLANs.	3
		<vlan-id>	Displays the status of the specified VLAN.	3
	vlan-stacking		Displays VLAN stacking settings.	3
	vlanlq	gvrp	Displays GVRP settings.	3
		port-isolation	Displays port isolation settings.	3
ssh	<1 2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.	0
		[command </>]	Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.	0
test	interface port-channel <port-list>		Performs an internal loopback test on the specified ports.	13
traceroute	<ip host-name> [in-band out-of-band vlan <vlan-id>][ttl <1-255>] [wait <1-60>] [queries <1-10>]		Determines the path a packet takes to a device.	0
	help		Displays help information for this command.	0

Table 138 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
write	memory		Saves current configuration to the configuration file the Switch is currently using.	13
		<index>	Saves current configuration to the specified configuration file on the Switch.	13

45.12.3 General Configuration Mode

The following table lists the commands in Configuration (or Config) mode.

Table 139 Command Summary: Configuration Mode

COMMAND			DESCRIPTION	PRIVILEGE
aaa	accounting	commands <privilege> stop-only tacacs+	Enables accounting of command sessions and specifies the minimum privilege level for which command sessions should be recorded.	13
		commands <privilege> stop-only tacacs+ [broadcast]	Enables sending accounting information for command sessions to all configured accounting servers at the same time.	13
		dot1x <start-stop stop-only> <radius tacacs+>	Enables accounting of IEEE 802.1x authentication sessions and specifies the mode and protocol method.	13
		dot1x <start-stop stop-only> <radius tacacs+> [broadcast]	Enables sending accounting information for IEEE 802.1x authentication sessions to all configured accounting servers at the same time.	13
		exec <start-stop stop-only> <radius tacacs+>	Enables accounting of administrative sessions via SSH, Telnet and console port and specifies the mode and protocol method.	13
		exec <start-stop stop-only> <radius tacacs+> [broadcast]	Enables sending accounting information for administrative sessions via SSH, Telnet and console port sessions to all configured accounting servers at the same time.	13
		system <radius tacacs+>	Enables accounting of system events and specifies the protocol method.	13
		system <radius tacacs+> [broadcast]	Enables sending accounting information for system events to all configured accounting servers at the same time.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		update periodic <1-2147483647>	Sets the update period for accounting sessions. This is the time the Switch waits to send an update to an accounting server after a session starts.	13
	authentication	enable <method1> [<method2> [<method3>]]	Enables authorization for executing commands on the Switch and specifies which method should be used first second and third. The methods can be, "enable", "radius" or "tacacs+"	14
		login <method1> [<method2> [<method3>]]	Enables authentication for administrative sessions on the Switch and specifies which method should be used first second and third. The methods can be, "local", "radius" or "tacacs+"	14
admin- password	<pw-string> <confirm-string>		Changes the administrator password.	14
arp inspection			Enables ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.	13
	filter-aging-time	<1-2147483647>	Specifies how long (1-2147483647 seconds) MAC address filters remain in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.	13
		none	Specifies the MAC address filter to be permanent.	13
	log buffer	entries <0-1024>	Specifies the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer.	13
		logs <0-1024> interval <0-86400>	Specifies the number of syslog messages that can be sent to the syslog server in one batch and how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server.	13
	vlan <vlan-list>		Enables ARP inspection on the specified VLAN(s).	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	logging [all none permit deny]	Enables logging of ARP inspection events on the specified VLAN(s). Optionally specifies which types of events to log.	13
bandwidth-control		Enables bandwidth control.	13
bcp-transparency		Enables Bridge Control Protocol (BCP) transparency.	13
classifier	<name> <[packet-format <802.3untag 802.3tag EtherIIuntag EtherIItag]> [priority <0-7>] [vlan <vlan-id>][ethernet-type <ether-num ip ipx arp rarp appletalk decnet sna netbios dlc>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [dscp <0-63>] [ip-protocol <protocol-num tcp udp icmp egp ospf rsvp igmp igmp pim ipsec> [establish-only]] [source-ip <src-ip-addr> [mask-bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask-bits>]] [destination-socket <socket-num>] [inactive]>	Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.	13
	help	Displays help information for this command.	13
cluster	<vlan-id>	Enables clustering in the specified VLAN group.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	member <mac-address> password <password-str>		Sets the cluster member.	13
	name <cluster name>		Sets a descriptive name for the cluster.	13
	rcommand <mac-address>		Logs into the CLI of the specified cluster member.	13
default-management	<in-band out-of-band>		Specifies through which traffic flow the Switch is to send packets.	13
dhcp	dhcp-vlan <vlan-id>		Specifies the VLAN ID for the DHCP VLAN.	13
dhcp	relay <vlan-id>	helper-address <remote-dhcp-server1>	Enables DHCP relay on the specified VLAN and sets the IP address of 1 DHCP server.	13
		helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>] [option] [information]	Enables DHCP relay on the specified VLAN and sets the IP address of up to 3 DHCP servers. Optionally sets the Switch to add relay agent information and system name.	13
	server <vlan-id>	starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253>	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration details to send to DHCP clients.	13
		starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253> [default-gateway <ip-addr>] [primary-dns <ip-addr>] [secondary-dns <ip-addr>]	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration details to send to DHCP clients. Including default gateway IP address and DNS server information.	13
	smart-relay		Enables DHCP relay for all broadcast domains on the Switch.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>]	Sets the IP addresses of up to 3 DHCP servers.	13
		information	Allows the Switch to add system name to agent information.	13
		option	Allows the Switch to add DHCP relay agent information.	13
dhcp	snooping		Enables DHCP Snooping on the Switch.	13
		database <tftp://host/ filename>	Specifies the location of the DHCP snooping database. The location should be expressed like this: tftp://{domain name or IP address}/directory, if applicable/ file name ; for example, tftp://192.168.10.1/database.txt .	13
		database timeout <seconds>	Specifies how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.	13
		database write- delay <seconds>	Specifies how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update.	13
		vlan <vlan- list>	Specifies the VLAN IDs for VLANs you want to enable DHCP snooping on.	13
		vlan <vlan- list> information	Sets the Switch to add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	13
		vlan <vlan- list> option	Sets the Switch to add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	13
diffserv			Enables DiffServ.	13
	dscp <0-63> priority <0-7>		Sets the DSCP-to-IEEE 802.1q mappings.	13
ethernet oam			Enables Ethernet OAM on the Switch.	13
exit			Exits from the CLI.	13
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
help			Displays help information.	0
history			Displays a list of previous command(s) that you have executed.	0
hostname	<name_string>		Sets the Switch's name for identification purposes.	13
https	cert-regeneration <rsa dsa>		Re-generates a certificate.	13
	timeout <0-65535>		Sets the HTTPS timeout period.	13
igmp-filtering			Enables IGMP filtering on the Switch.	13
	profile <name> start-address <ip> end-address <ip>		Sets the range of multicast address(es) in a profile.	13
igmp-snooping			Enables IGMP snooping.	13
	8021p-priority	<0-7>	Sets the 802.1p priority for outgoing igmp snooping packets.	13
	host-timeout	<1-16711450>	Sets the host timeout value.	13
	leave-timeout	<1-16711450>	Sets the leave timeout value	13
	unknown-multicast-frame <drop flooding>		Sets how to treat traffic from unknown multicast group.	13
	reserved-multicast-group <drop flooding>		Sets how to treat traffic belonging to reserved multicast groups.	13
	vlan	<vlan-id>	Specifies which VLANs to perform IGMP snooping on.	13
		<vlan-id> [name <name>]	Allows you to set a name for a multicast VLAN.	13
		mode <auto fixed>	Specifies whether the Switch should automatically learn the first 16 VLAN's that send multicast traffic via the Switch (auto) or whether the Switch will only perform IGMP snooping on the VLANs configured on the Switch.	13
interface	port-channel <port-list>		Enables a port or a list of ports for configuration. See Section 45.12.4 on page 368 for more details.	13
	route-domain <ip-address>/<mask-bits>		Enables a routing domain for configuration. See Section 45.12.5 on page 373 for more details.	13
ip	address	<ip> <mask>	Sets the IP address and subnet mask of the out-of-band management port.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		default-gateway <ip>	Sets the default gateway's IP address for the out-of-band management port.	13
	name-server	<ip>	Sets the IP address of a domain name server.	13
	route	<ip> <mask> <next-hop-ip>	Creates a static route.	13
		<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]	Sets the metric of a static route or deactivates a static route.	13
	source binding <mac-addr> vlan <vlan-id> <ip>		Creates a static binding for DHCP snooping and ARP inspection.	13
		interface port- channel <interface-id>	Specifies the port(s) for this static binding.	13
lacp			Enables Link Aggregation Control Protocol (LACP).	13
	system-priority	<1-65535>	Sets the priority of an active port using LACP.	13
logins	username <name> password <pwd>		Configures up to four read-only login accounts.	14
	username <name>	privilege <0-14>	Assigns a privilege level to user accounts.	14
logout			Exits from the CLI.	0
loopguard			Enables loopguard on the Switch.	13
mac-authentication			Enables MAC authentication on the Switch.	13
	nameprefix <name-string>		Sets the prefix appended to the MAC address before it is sent to the RADIUS server for authentication.	13
	password <name-string>		Sets the password sent to the RADIUS server for clients using MAC authentication.	13
	timeout <1-3000>		Specifies the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. This settings is superseded by the mac-aging-time command.	13
mac-aging-time	<10-3000>		Sets learned MAC aging time.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>		Configures a static MAC address port filtering rule.	13
		inactive	Disables a static MAC address port filtering rule.	13
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.	13
		inactive	Disables a static MAC address forwarding rule.	13
mirror-port			Enables port mirroring.	13
	<port-num>		Enables port mirroring on a specified port.	13
mode	zynos		Changes the CLI mode to the ZyNOS format.	13
mrstp	<tree-index>		Activates the specified STP configuration.	13
		priority <0-61440>	Sets the priority for the specified tree.	13
		hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets hello-time, maximum-age and forward delay for the specified tree.	13
	interface <port-list>		Activates STP on the specified ports.	13
		path-cost <1-65535>	Sets a path cost to the specified ports.	13
		priority <0-255>	Sets the priority value to the specified ports for STP.	13
		tree-index <1-4>	Assigns a specific STP configuration to the ports.	13
	help		Displays the detailed help for the mrstp command.	13
mstp			Activates MSTP on the Switch.	13
	configuration name		Sets a name for an MSTP region.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.	13
	instance <0-16>		Specifies which MST instance you are configuring.	13
		interface port-channel <port-list>	Specifies the ports you want to participate in this MST instance.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		interface port-channel <port-list> path-cost <1-65535>	Assigns the path cost to the specified ports.	13
		interface port-channel <port-list> priority <1-255>	Assigns priority to the specified ports.	13
	max-hop <1-255>		Sets the maximum hop value before BPDUs are discarded in the MST Region.	13
	revision <0-65535>		Sets the revision number for this MST Region configuration.	13
multi-login			Enables multi-login.	14
mvr	<vlan-id>		Enters the MVR (Multicast VLAN Registration) configuration mode. Refer to Section 45.13 on page 376 for more information.	13
no	aaa accounting	commands	Disables accounting of command sessions on the Switch.	13
		dot1x	Disables accounting of IEEE 802.1x authentication sessions on the Switch.	13
		exec	Disables accounting of administrative sessions via SSH, Telnet or console on the Switch.	13
		system	Disables accounting of system events on the Switch.	13
		update	Resets the accounting update interval to the value "0".	13
	aaa authentication	enable	Disables authorization of executing commands on the Switch.	13
		login	Disables authentication of administrative sessions on the Switch.	13
	arp inspection		Disables ARP inspection on the Switch.	13
		filter-aging-time	Resets how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet to the default value (300 seconds).	13
		log-buffer entries	Resets the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server to the default value (3).	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		log-buffer logs	Resets the maximum number of syslog messages the Switch can send to the syslog server in one batch to the default value (4).	13
		vlan <vlan-list>	Disables ARP inspection on the specified VLAN(s).	13
		vlan <vlan-list> logging	Disables logging of messages generated by ARP inspection for the specified VLAN(s).	13
	bandwidth-control		Disable bandwidth control on the Switch.	13
	bcp-transparency		Disables Bridge Control Protocol Transparency	13
	classifier	<name>	Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.	13
		<name> inactive	Enables a classifier.	13
	cluster		Disables cluster management on the Switch.	13
		member <mac-address>	Removes the cluster member.	13
	dhcp relay		Disables DHCP relay.	13
		information	Disables the relay agent information option 82.	13
		option	System name is not appended to option 82 information field.	13
	dhcp server <vlan-id>		Disables DHCP server settings.	13
		default-gateway	Disables DHCP server default gateway settings.	13
		primary-dns	Disables DHCP primary DNS server settings.	13
		secondary-dns	Disables DHCP server secondary DNS settings.	13
	dhcp smart relay		Disables global DHCP relay settings.	13
		information	Disables the relay agent information option 82 for global dhcp settings.	13
		option	System name is not appended to option 82 information field for global dhcp settings..	13
	dhcp snooping		Disables DHCP Snooping on the Switch.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		vlan <vlan-list>	Specifies the VLAN IDs for VLANs you want to disable DHCP snooping on.	13
		vlan <vlan-list> information	Sets the Switch to not add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	13
		vlan <vlan-list> option	Sets the Switch to not add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	13
		database	Removes the location of the DHCP snooping database.	13
		database timeout	Resets how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up to the default value (300).	13
		database write-delay	Resets how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update to the default value (65535).	13
	dhcp dhcp-vlan		Disables DHCP VLAN on the Switch.	13
	diffserv		Disables DiffServ on the Switch.	13
	ethernet oam		Disables Ethernet OAM on the Switch.	13
	igmp-filtering		Disables IGMP filtering on the Switch.	13
		profile <name>	Removes the specified IGMP filtering profile.	13
		profile <name> start-address <ip> end-address <ip>	Clears the settings of the specified IGMP filtering profile.	13
	igmp-snooping		Disables IGMP snooping.	13
		8021p-priority	Disables changing the priority of outgoing IGMP control packets.	13
		vlan <vlan-id>	Removes IGMP snooping configuration on the specified VLAN.	13
	ip		Sets the management IP address to the default value.	13
		route <ip> <mask>	Removes a specified IP static route.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		route <ip> <mask> inactive	Enables a specified IP static route.	13
	lacp		Disables the link aggregation control protocol (dynamic trunking) on the Switch.	13
	logins <name>		Disables login access to the specified name.	14
	loopguard		Disables loopguard on the Switch.	13
	mac-authentication		Disables MAC authentication on the Switch.	13
	mac-authentication timeout		Resets the MAC authentication timeout value on the Switch to "0".	13
	mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both> inactive	Enables the specified MAC-filter rule.	13
		name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both>	Disables the specified MAC filter rule.	13
	mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>	Removes the specified MAC forwarding entry, belonging to a VLAN group (if any) forwarded through an interface(s).	13
		name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive	Enables the specified MAC address, belonging to a VLAN group (if any) forwarded through an interface(s).	13
	mirror-port		Disables port mirroring on the Switch.	13
	mrstp	<treeIndex>	Disables the specified STP configuration.	13
	mrstp	interface <port-list>	Disables the STP assignment from the specified port(s).	13
	mstp		Disables MSTP on the Switch.	13
		<instance> <0-16>	Disables the specified MST instance on the Switch.	13
		<instance> <0-16> vlan <1-4094>	Disables the assignment of specific VLANs from an MST instance.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		instance <0-16> interface port-channel <port-list>	Disables the assignment of specific ports from an MST instance.	13
	multi-login		Disables another administrator from logging into Telnet or the CLI.	14
	mvr <vlan-id>		Removes an MVR configuration from the Switch.	13
	password privilege <0-14>		Disables a password to execute commands of the specified privilege level.	14
	policy <name>		Deletes the policy. A policy sets actions for the classified traffic.	13
		inactive	Enables a policy.	13
	port-access-authenticator		Disables port authentication on the Switch.	13
		<port-list>	Disables authentication on the listed ports.	13
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).	13
	port-security		Disables port security on the device.	13
		<port-list>	Disables port security on the specified ports.	13
		<port-list> learn inactive	Enables MAC address learning on the specified ports.	13
	radius-accounting	<index>	Disables accounting on the specified RADIUS server.	13
	radius-server	<index>	Disables the use of authentication from the specified RADIUS server.	13
	remote-management	<index>	Clears a secure client set entry from the list of secure clients.	13
		<index> service <telnet ftp http icmp snmp ssh https>	Disables a secure client set entry number from using the selected remote management service.	13
	router	dvmrp	Disables DVMRP on the Switch.	13
		igmp	Disables IGMP on the Switch.	13
		ospf	Disables OSPF on the Switch.	13
		rip	Disable RIP on the Switch.	13
		vrrp network <ip-address>/ <mask-bits> vr-id <1-7>	Deletes VRRP settings.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	service-control	ftp	Disables FTP access to the Switch.	13
		http	Disables web browser control to the Switch.	13
		https	Disables secure web browser access to the Switch.	13
		icmp	Disables ICMP access to the Switch such as pinging and tracerouting.	13
		snmp	Disables SNMP management.	13
		ssh	Disables SSH (Secure Shell) server access to the Switch.	13
		telnet	Disables telnet access to the Switch.	13
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.	13
		enable traps	Disables all SNMP traps from being sent to a manager.	13
		enable traps aaa	Disables sending all AAA type traps to a manager.	13
		enable traps aaa <options>	Disables sending specific AAA traps to a manager. The options are "authentication" or "accounting".	13
		enable traps interface	Disables sending all interface type traps to a manager.	13
		enable traps interface <options>	Disables sending all interface type traps to a manager. The options are "linkup", "linkdown" and "autonegotiation".	13
		enable traps ip	Disables sending all IP type traps to a manager.	13
		enable traps ip <options>	Disables sending all IP type traps to a manager. The options are "ping" or "traceroute".	13
		enable traps switch	Disables sending all Switch type traps to a manager.	13
		enable traps switch <options>	Disables sending all Switch type traps to a manager. The options are "stp", "mactable" or "rmon".	13
		enable traps system	Disables sending all system type traps to a manager.	13
		enable traps system <options>	Disables sending all system type traps to a manager. The options are "coldstart", "warmstart", "fanspeed", "temperature", "voltage", "reset", "timesync", "intrusionlock" or "loopguard".	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	spanning-tree		Disables STP.	13
		<port-list>	Disables STP on listed ports.	13
	ssh	key <rsa1 rsa dsa>	Disables the secure shell server encryption key. Your Switch supports SSH versions 1 and 2 using RSA and DSA authentication.	13
		known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.	13
		known-hosts <host-ip> [1024 ssh- rsa ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).	13
	storm-control		Disables broadcast storm control.	13
	subnet-based-vlan		Disables subnet based VLAN on the Switch.	13
		source-ip <ip> mask-bits <mask-bits>	Removes the specified subnet from the subnet based VLAN configuration.	13
		dhcp-vlan- override	Disables the DHCP VLAN override setting for subnet based VLAN(s).	13
	syslog		Disables syslog logging.	13
		server <ip- address>	Disables syslog logging to the specified syslog server.	13
		server <ip- address> inactive	Enables syslog logging to the specified syslog server.	13
		type [type]	Disables syslog logging for the specified log type (sys, link, config, error or report).	13
	tacacs-accounting	<index>	Disables TACACS+ accounting on the specified server.	13
	tacacs-server	<index>	Disables TACACS+ authentication on the specified server.	13
	time	daylight- saving-time	Disables daylight saving on the Switch.	13
	timesync		Disables timeserver settings.	13
	trtcm		Disables the Two Rate Three Color Marker feature on the Switch.	13
	trunk	<T1 T2 T3 T4 T5 T6>	Disables the specified trunk group.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		<T1 T2 T3 T4 T5 T6> interface <port-list>	Removes ports from the specified trunk group.	13
		<T1 T2 T3 T4 T5 T6> lacp	Disables LACP in the specified trunk group.	13
	vlan	<vlan-id>	Deletes the static VLAN entry.	13
	vlan1q	gvrp	Disables GVRP on the Switch.	13
		port-isolation	Disables port isolation.	13
	vlan-stacking		Disables VLAN stacking.	13
password	<password>		Changes the password for the highest privilege level.	14
password	<password>	privilege <0-14>	Changes the password for the specified privilege.	14

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
policy	<name> classifier <classifier-list> < [vlan<vlan-id>] [egress-port <port-num>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <bandwidth>] [outgoing-packet-format <tagged untagged>] [out-of-profile-dscp <0-63>] [forward-action <drop forward>] [queue-action <prio-set prio-queue prio-replace-tos>] [diffserv-action <diff-set-tos diff-replace-priority diff-set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non-unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile-action <[change-dscp][drop][forward] [set-drop-precedence]>] [inactive]>		Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.	13
port-access-authenticator			Enables 802.1x authentication on the Switch.	13
	<port-list>		Enables 802.1x authentication on the specified port(s).	13
		reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	13
		reauth-period <reauth-period>	Specifies how often a client has to re-enter the username and password to stay connected to the specified port(s).	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
port-security			Enables port security on the device.	13
	<port-list>		Enables port security on the specified port(s).	13
		learn inactive	Disables MAC address learning on the specified port(s).	13
		address-limit <number>	Limits the number of (dynamic) MAC addresses that may be learned on a port.	13
		MAC-freeze	Adds learned MAC addresses to the static MAC table and stops learning any more MAC addresses.	13
queue	priority <0-7> level <0-7>		Sets the priority level-to-physical queue mapping.	13
radius-accounting	host <index><ip>		Specifies the IP address of RADIUS accounting server 1 or RADIUS accounting server 2 (index =1 or index =2).	13
		[acct-port <socket-number>] [key <key-string>]	Sets the port number and key of the external RADIUS accounting server.	13
	timeout <1-1000>		Specifies the RADIUS accounting server timeout value.	13
radius-server	host <index> <ip>		Specifies the IP address of RADIUS server 1 or RADIUS server 2 (index =1 or index =2).	13
		[auth-port <socket-number>] [key <key-string>]	Sets the port number and key of the external RADIUS server.	13
	timeout <1-1000>		Specifies the RADIUS server timeout value.	13
	mode	<index-priority round-robin>	Specifies the mode for RADIUS server selection.	13
remote-management	<index> start-addr <ip> end-addr <ip> service <telnet ftp http icmp snmp>		Specifies a group of trusted computer(s) from which an administrator may use a service to manage the Switch.	13
router	dvmrp		Enables and enters the DVMRP configuration mode.	13
		exit	Leaves the DVMRP configuration mode.	13
		threshold <ttl-value>	Sets the DVMRP threshold value.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	igmp		Enables and enters the IGMP configuration mode.	13
		exit	Leaves the IGMP configuration mode.	13
		non-querier	Sets the Switch to Non-Querier mode. (If a multicast router with a lower IP address, it will stop sending Query messages on that network.)	13
		no non-querier	Disables non-querier mode on the Switch, (a multicast router always sends Query messages).	13
		unknown-multicast-frame <drop flooding>	Specifies the action the Switch should perform when it receives unknown multicast frames.	13
	ospf <router-id>		Enables and enters the OSPF configuration mode.	13
		area <area-id>	Enables and sets the area ID.	13
		area <area-id> authentication	Enables simple authentication for the area.	13
		area <area-id> authentication message-digest	Enables MD5 authentication for the area.	13
		area <area-id> default-cost <0-16777214>	Sets the cost to the area.	13
		area <area-id> name <name>	Sets a descriptive name for the area for identification purposes.	13
		area <area-id> stub	Enables and sets the area as a stub area.	13
		area <area-id> stub no-summary	Sets the stub area not to send any LSA (Link State Advertisement).	13
		area <area-id> virtual-link <router-id>	Sets the virtual link ID information for the area.	13
		area <area-id> virtual-link <router-id> authentication- key <key>	Enables simple authentication and sets the authentication key for the specified virtual link in the area.	13
		area <area-id> virtual-link <router-id> authentication- same-as-area	Sets the virtual link to use the same authentication method as the area.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		area <area-id> virtual-link <router-id> message-digest- key <keyid> md5 <key>	Enables MD5 authentication and sets the key ID and key for the virtual link in the area.	13
		area <area-id> virtual-link <router-id> name <name>	Sets a descriptive name for the virtual link for identification purposes.	13
		exit	Leaves the router OSPF configuration mode.	13
		network <ip- addr/bits> area <area-id>	Creates an OSPF area.	13
		no area <area- id>	Removes the specified area.	13
		no area <area- id> authentication	Sets the area to use no authentication (None).	13
		no area <area- id> default- cost	Sets the area to use the default cost (15).	13
		no area <area- id> stub	Disables stub network settings in the area.	13
		no area <area- id> stub no- summary	Sets the area to send LSAs (Link State Advertisements).	13
		no area <area- id> virtual- link <router- id> authentication- key	Resets the authentication settings on this virtual link.	13
		no area <area- id> virtual- link <router- id> message- digest-key	Resets the authentication settings on this virtual link.	13
		no area <area- id> virtual- link <router- id> authentication- same-as-area	Resets the authentication settings on this virtual area.	13
		no area <area- id> virtual- link <router- id>	Deletes the virtual link from the area.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		no network <ip-addr/bits>	Deletes the OSPF network.	13
		no redistribute rip	Sets the Switch not to learn RIP routing information.	13
		no redistribute static	Sets the Switch not to learn static routing information.	13
		redistribute rip metric-type <1 2> metric <0-65535>	Sets the Switch to learn RIP routing information which will use the specified metric information.	13
		redistribute static metric-type <1 2> metric <0-65535>	Sets the Switch to learn static routing information which will use the specified metric information.	13
		passive-iface <ip-addr/bits>	Sets the interface to be passive. A passive interface does not send or receive OSPF traffic.	13
	rip		Enables and enters the RIP configuration mode.	13
		exit	Leaves the RIP configuration mode.	13
	vrrp network <ip-address>/<mask-bits> vr-id <1-7> uplink-gateway <ip>		Adds a new VRRP network and enters the VRRP configuration mode.	13
		exit	Exits from the VRRP command mode.	13
		inactive	Disables the VRRP settings.	13
		interval <1..255>	Sets the time interval (in seconds) between Hello message transmissions.	13
		name <name string>	Sets a descriptive name of the VRRP setting for identification purposes.	13
		no inactive	Activates this VRRP.	13
		no preempt	Disables VRRP preemption mode.	13
		no primary-virtual-ip	Resets the network to use the default primary virtual gateway (interface IP address).	13
		no secondary-virtual-ip	Sets the network to use the default secondary virtual gateway (0.0.0.0).	13
		preempt	Enables preemption mode.	13
		primary-virtual-ip <ip>	Sets the primary VRRP virtual gateway IP address.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		priority <1-254>	Sets the priority of the uplink-gateway.	13
		secondary-virtual-ip <ip>	Sets the secondary VRRP virtual gateway IP address.	13
service-control	ftp <socket-number>		Allows FTP access on the specified service port.	13
	http <socket-number> <timeout>		Allows HTTP access on the specified service port and defines the timeout period.	13
	https <socket-number>		Allows HTTPS access on the specified service port.	13
	icmp		Allows ICMP management packets.	13
	snmp		Allows SNMP management.	13
	ssh <socket-number>		Allows SSH access on the specified service port.	13
	telnet <socket-number>		Allows Telnet access on the specified service port.	13
snmp-server	[contact <system contact>] [location <system location>]		Sets the geographic location and the name of the person in charge of this Switch.	13
	get-community <property>		Sets the get community.	13
	set-community <property>		Sets the set community.	13
	trap-community <property>		Sets the trap community.	13
	trap-destination <ip>		Sets the IP addresses of up to four stations to send your SNMP traps to.	13
	trap-destination <ip>	[udp-port <socket-number>] [version <v1v2cv3>][username <name>]	Sets the IP address of an SNMP manager. You can configure up to four managers to send your SNMP traps to.	13
	trap-destination <ip> enable traps		Enables sending SNMP traps to a manager.	13
		aaa	Enables sending all AAA type traps to a manager.	13
		aaa <options>	Enables sending specific AAA traps to a manager. The options are "authentication" or "accounting".	13
		help	Displays help information for SNMP trap commands.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		interface	Enables sending all interface type traps to a manager.	13
		interface <options>	Enables sending all interface type traps to a manager. The options are "linkup", "linkdown" and "autonegotiation".	13
		ip	Enables sending all IP type traps to a manager.	13
		ip <options>	Enables sending all IP type traps to a manager. The options are "ping" or "traceroute".	13
		switch	Enables sending all Switch type traps to a manager.	13
		switch <options>	Enables sending all Switch type traps to a manager. The options are "stp", "mactable" or "rmon".	13
		system	Enables sending all system type traps to a manager.	13
		system <options>	Enables sending all system type traps to a manager. The options are "coldstart", "warmstart", "fanspeed", "temperature", "voltage", "reset", "timesync", "intrusionlock" or "loopguard".	13
	username <name>	sec-level <noauth auth priv>	Sets the authentication level for SNMP v3 user authentication.	13
		sec-level <noauth auth priv> [auth <md5sha>][priv <des aes>]	Specifies the authentication and encryption methods for communication with the SNMP manager.	13
	version <v2c v3 v3v2c>		Sets the SNMP version to use for communication with the SNMP manager.	13
spanning-tree			Enables STP on the Switch.	13
	mode <RSTP MRSTP MSTP>		Specifies the STP mode you want to implement on the Switch.	13
	<port-list>		Enables STP on a specified port.	13
	<port-list> path-cost <1-65535>		Sets the STP path cost for a specified port.	13
	<port-list> priority <0-255>		Sets the priority for a specified port.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.	13
	help		Displays help information.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	priority <0-61440>		Sets the bridge priority of the Switch.	13
ssh	known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>		Adds a remote host to which the Switch can access using SSH service.	13
storm-control			Enables broadcast storm control on the Switch.	13
subnet-based-vlan			Enables subnet based VLAN on the Switch.	13
	dhcp-vlan-override		Sets the Switch to force the DHCP clients to obtain their IP addresses through the DHCP VLAN.	13
	name <name> source-ip <ip> mask-bits <mask-bits> vlan <vid> priority <0-7>		Specifies the name, IP address, subnet mask, VLAN ID of the subnet based VLAN you want to configure along with the priority you want to assign to the outgoing frames for this VLAN.	13
		inactive	Disables the subnet based VLAN.	13
syslog			Enables syslog logging.	13
	server <ip-address>	inactive	Disables syslog logging to the specified syslog server.	13
		level [0 ~ 7]	Sets the IP address of the syslog server and the severity level.	13
	type <type> facility [local 1 ..7]		Sets the log type and the file location on the syslog server.	13
tacacs-accounting	host <index><ip>		Specifies the IP address of TACACS+ accounting server 1 or TACACS+ accounting server 2 (index = 1 or index = 2).	13
		[acct-port <socket-number>] [key <key-string>]	Sets the port number and key of the external TACACS+ accounting server.	13
	timeout <1-1000>		Specifies the TACACS+ accounting server timeout value.	13
tacacs-server	host <index> <ip>		Specifies the IP address of TACACS+ server 1 or TACACS+ server 2 (index = 1 or index = 2).	13
		[auth-port <socket-number>] [key <key-string>]	Sets the port number and key of the external TACACS+ server.	13
	timeout <1-1000>		Specifies the TACACS+ server timeout value.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	mode	<index-priority round-robin>	Specifies the mode for TACACS+ server selection.	13
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.	13
	date <month/day/year>		Sets the date in year, month and day format.	13
	daylight-saving-time		Enables daylight saving time.	13
		end-date <week> <day> <month> <o'clock>	Sets the day and time when Daylight Saving Time ends.	13
		help	Displays help for the daylight-saving-time command.	13
		start-date <week> <day> <month> <o'clock>	Sets the day and time when Daylight Saving Time starts.	13
	help		Displays help information.	13
	timezone <-1200 ... 1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.	13
timesync	<daytime time ntp>		Sets the time server protocol.	13
	server <ip>		Sets the IP address of your time server.	13
trtcm			Enables Two Rate Three Color Marker on the Switch.	13
	mode <color-aware color-blind>		Sets the mode for Two Rate Three Color Marker on the Switch.	13
trunk	<T1 T2 T3 T4 T5 T6>		Activates a trunk group.	13
	<T1 T2 T3 T4 T5 T6> >lacp		Enables LACP for a trunk group.	13
	<T1 T2 T3 T4 T5 T6> >interface <port-list>		Adds a port(s) to the specified trunk group.	13
	interface <port-list> timeout <lacp-timeout>		Defines the port number and LACP timeout period.	13
vlan	<vlan-id>		Enters the VLAN configuration mode. See Section 45.12.6 on page 375 for more information.	13
vlanlq	gvrp		Enables GVRP.	13
	port-isolation		Enables port-isolation.	13
vlan-stacking			Enables VLAN stacking on the Switch.	13

Table 139 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	<SPTPID>		Sets the SP TPID (Service Provider Tag Protocol Identifier).	13
vlan-type	<802.1q port-based>		Specifies the VLAN type.	13

45.12.4 interface port-channel Commands

The following table lists the `interface port-channel` commands in configuration mode. Use these commands to configure the ports.

Table 140 interface port-channel Commands

COMMAND			DESCRIPTION	PRIVILEGE
interface port-channel <port-list>			Enables a port or a list of ports for configuration.	13
	arp inspection	trust	Sets the port to be a trusted port for arp inspection. The Switch does not discard ARP packets on trusted ports for any reason.	13
		limit rate <pps>	Specifies the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.	13
		limit rate <pps> burst interval <seconds>	Specifies the length (1-15 seconds) of the burst interval. The burst interval is the length of time over which the rate of ARP packets is monitored for each port.	13
	bandwidth-limit		Enables ingress (pir), cir and egress limits on the port(s).	13
		cir	Enables the guaranteed bandwidth limits for incoming traffic on the port(s).	13
		cir <Kbps>	Sets the guaranteed bandwidth allowed for incoming traffic on the port(s).	13
		pir	Enables bandwidth limits allowed for incoming traffic on the port(s).	13
		pir <Kbps>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	13
		egress	Enables bandwidth limits allowed for outgoing traffic on the port(s).	13

Table 140 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		egress <Kbps>	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	13
	bpdu-control <peer tunnel discard network>		Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states.	13
	broadcast-limit		Enables broadcast storm control limit on the port(s).	13
		<pkt/s>	Specifies the maximum number of broadcast packets to allow through the port.	13
	dhcp snooping trust		Sets this port as a trusted DHCP snooping port. Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.	13
	dhcp snooping limit rate <pps>		Sets the maximum rate that DHCP packets are allowed to arrive at a trusted DHCP snooping port.	13
	diffserv		Enables DiffServ on the port(s).	13
	dlf-limit		Enables the Destination Lookup Failure (DLF) limit.	13
		<pkt/s>	Sets the interface DLF limit in packets per second (pps).	13
	egress set <port-list>		Sets the outgoing traffic port list for a port-based VLAN.	13
	ethernet oam		Enables Ethernet OAM on the port(s).	13
		mode <active passive>	Specifies active or passive OAM mode on the ports. Active mode allows the port to issue remote loopback and discovery commands. Passive mode means that the port can only respond to Ethernet OAM commands.	13
		remote-loopback supported	Enable Ethernet OAM remote-loopback capability on the port(s).	13
	exit		Exits from the interface port-channel command mode.	13
	flow-control		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	13
	frame-type <all tagged untagged>		Choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.	13

Table 140 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	ge-spq	<q0 q1 ... q7>	Enables strict priority queuing starting with the specified queue and subsequent higher queues on the Gigabit ports.	13
	gvrp		Enables this function to permit VLAN groups beyond the local Switch.	13
	help		Displays a description of the interface port-channel commands.	13
	igmp-filtering	profile <name>	Applies the specified IGMP filtering profile.	13
	igmp-group-limited		Enables the IGMP group limiting feature.	13
		number <number>	Sets the maximum number IGMP groups allowed.	13
	igmp-immediate-leave		Enables the IGMP immediate leave function.	13
	igmp-querier-mode <auto fixed edge>		Sets the IGMP query mode for the port.	13
	inactive		Disables the specified port(s) on the Switch.	13
	ingress-check		Enables the device to discard incoming frames for VLANs that are not included in a port member set.	13
	intrusion-lock		Enables intrusion lock on the port(s) and a port cannot be connected again after you disconnected the cable.	13
	ipmc egress-untag-vlan <vlan-id>		Enables the port(s) to remove specified VLAN tag from IP multicasting packets before forwarding.	13
	loopguard		Enables the loopguard feature on the port(s).	13
	mac-authentication		Enables MAC authentication via a RADIUS server on the port(s).	13
	mirror		Enables port mirroring in the interface.	13
		dir <ingress egress both>	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.	13
	multicast-limit		Enables the port(s) multicast limit.	13
		<pkt/s>	Sets how many multicast packets the port(s) receives per second.	13

Table 140 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	name <port-name-string>		Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).	13
	no	arp inspection trust	Disables this port from being a trusted port for ARP inspection.	13
		arp inspection limit	Resets the ARP inspection rate to the default (0).	13
		bandwidth-limit	Disables bandwidth limit on the port(s).	13
		bandwidth-limit <cir>	Disables cir bandwidth limits on the port(s).	13
		bandwidth-limit <pir>	Disables pir bandwidth limits on the port(s).	13
		bandwidth-limit <egress>	Disables egress bandwidth limits on the port(s).	13
		broadcast-limit	Disables broadcast storm control limit on the port(s).	13
		dhcp snooping trust	Disables this port from being a trusted port for DHCP snooping.	13
		dhcp snooping limit rate	Resets the DHCP snooping rate to the default (0).	13
		diffserv	Disables DiffServ on the port(s).	13
		dlf-limit	Disables destination lookup failure (DLF) on the Switch.	13
		egress-set <port-list>	Disables the egress port setting.	13
		ethernet oam	Disables Ethernet OAM on the port(s).	13
		ethernet oam mode	Resets Ethernet OAM mode to the default setting (active) on the ports.	13
		ethernet oam remote-loopback supported	Disables Ethernet OAM remote loop-back capability on the port(s).	13
		flow-control	Disables flow control on the port(s).	13
		ge-spq	Disables strict priority queuing on the Gigabit ports.	13
		gvrp	Disable GVRP on the port(s).	13
		igmp-filtering profile	Disables IGMP filtering.	13
		igmp-group-limit	Disables IGMP group limitation.	13
		igmp-immediate-leave	Disables the IGMP immediate leave function.	13
		inactive	Enables the port(s) on the Switch.	13

Table 140 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		ingress-check	Disables ingress checking on the port(s).	13
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	13
		ipmc egress-untag-vlan <vlan-id>	Disables the port(s) from removing specified VLAN tag from IP multicasting packets before forwarding.	13
		loopguard	Disables the loop guard feature on the port(s).	13
		mac-authentication	Disables MAC authentication via a RADIUS server on the port(s).	13
		mirror	Disables port mirroring on the port(s).	13
		multicast-limit	Disables multicast limit on the port(s).	13
		trtcm	Disables 2-rate 3-color marking on the port(s).	13
		vlan-trunking	Disables VLAN trunking on the port(s).	13
	pvid <vlan-id>		The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	13
	qos	priority <0 .. 7>	Sets the quality of service priority for an interface.	13
	speed-duplex	<auto 10-half 10-full 100-half 100-full 1000-full>	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.	13
	spq		Sets the port(s) to use Strict Priority Queuing.	13
	trtcm		Enables Two Rate Three Color Marker on the port(s).	13
		cir <Kbps>	Sets the Commit Information Rate on the port(s).	13
		pir <Kbps>	Sets the Peak Information Rate on the port(s).	13
		dscp green <0-63>	DSCP value to use for packets with low packet loss priority.	13
		dscp yellow <0-63>	DSCP value to use for packets with medium packet loss priority.	13
		dscp red <0-63>	DSCP value to use for packets with high packet loss priority.	13

Table 140 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	vlan-stacking	priority <0-7>	Sets the priority of the specified port(s) in VLAN stacking.	13
		role <access tunnel>	Sets the VLAN stacking port roles of the specified port(s).	13
		SPVID <vlan-id>	Sets the service provider VID of the specified port(s).	13
	vlan-trunking		Enables VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.	13
	weight <wt1> <wt2> ... <wt8>		A weight value of one to eight is given to each variable from wt 1 to wt 8.	13
	wrr		Sets the port(s) to use Weighted Round Robin queuing.	13

45.12.5 interface route-domain Commands

The following table lists the `interface route-domain` commands in configuration mode.

Use these commands to configure the IP routing domains.

Table 141 interface route-domain Commands

COMMAND			DESCRIPTION	PRIVILEGE
interface route-domain <ip-address>/ <mask-bits>			Enables a routing domain for configuration.	13
	exit		Exits from the interface routing-domain command mode.	13
	ip	dvmrp	Enables this function to permit VLAN groups beyond the local Switch.	13
		igmp <v1 v2 v3>	Enables IGMP in this routing domain and specifies the version of the IGMP packets that the Switch should use.	13
		igmp robustness-variable <2-255>	Sets the igmp robustness variable on the Switch. This variable specifies how susceptible the subnet is to lost packets.	13
		igmp query-interval	Sets the igmp query interval on the Switch. This variable specifies the amount of time in seconds between general query messages sent by the router.	13

Table 141 interface route-domain Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		igmp query-max-response-time <1-25>	Sets the maximum time that the router waits for a response to an general query message.	13
		igmp last-member-query-interval <1-25>	Sets the amount of time in seconds that the router waits for a response to a group specific query message.	13
		ospf authentication-key <k>	Enables OSPF authentication in this routing domain.	13
		ospf authentication-same-as-area	Sets the same OSPF authentication settings in the routing domain as the associated area.	13
		ospf cost <1-65535>	Sets the OSPF cost in this routing domain.	13
		ospf message-digest-key <k>	Sets the OSPF authentication key in this routing domain.	13
		ospf priority <0-255>	Sets the OSPF priority for the interface. Setting this value to 0 means that this router will not participate in router elections.	13
		rip direction <Outgoing Incoming Both None> version <v1 v2b v2m>	Sets the RIP direction in this routing domain as well as the version number.	13
		vrrp authentication-key <k>	Sets the VRRP authentication key in the routing domain.	13
	no	ip dvmrp	Disables DVMRP in this routing domain.	13
		ip igmp	Disables IP IGMP in this routing domain.	13
		ip ospf authentication-key	Disables OSPF authentication key settings in this routing domain.	13
		ip ospf authentication-same-as-area	Sets the routing domain not to use the same OSPF authentication settings as the area.	13
		ip ospf cost	Disables the OSPF cost in the routing domain.	13
		ip ospf message-digest-key	Sets the routing domain not to use a security key in OSPF.	13
		ip ospf priority	Resets the OSPF priority for the interface.	13
		ip vrrp authentication-key	Resets the VRRP authentication settings.	13

45.12.6 config-vlan Commands

The following table lists the `vlan` commands in configuration mode.

Table 142 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION	PRIVILEGE
<code>vlan</code> <code><vlan-id></code>			Creates a new VLAN group.	13
	<code>exit</code>		Leaves the VLAN configuration mode.	13
	<code>fixed <port-list></code>		Specifies the port(s) to be a permanent member of this VLAN group.	13
	<code>forbidden <port-list></code>		Specifies the port(s) you want to prohibit from joining this VLAN group.	13
	<code>help</code>		Displays a list of available VLAN commands.	13
	<code>inactive</code>		Disables the specified VLAN.	13
	<code>ip address</code>	<code><ip-address> <mask></code>	Sets the IP address of the Switch in the VLAN.	13
		<code><ip-address> <mask></code> <code>manageable</code>	Sets the IP address of the Switch in the VLAN and allow remote management to this IP address.	13
		<code>default-gateway <ip-address></code>	Sets the default gateway IP address in this VLAN.	13
	<code>name <name-str></code>		Specifies a name for identification purposes.	13
	<code>no</code>	<code>fixed <port-list></code>	Sets fixed port(s) to normal port(s).	13
		<code>forbidden <port-list></code>	Sets forbidden port(s) to normal port(s).	13
		<code>inactive</code>	Enables the specified VLAN.	13
		<code>ip address <ip-address> <mask></code>	Deletes the IP address and subnet mask from this VLAN.	13
		<code>ip address default-gateway</code>	Deletes the default gateway from this VLAN.	13
		<code>untagged <port-list></code>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.	13
	<code>normal <port-list></code>		Specifies the port(s) to dynamically join this VLAN group using GVRP	13
	<code>untagged <port-list></code>		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	13

45.13 mvr Commands

The following table lists the mvr commands in configuration mode.

Table 143 Command Summary: mvr Commands

COMMAND			DESCRIPTION	PRIVILEGE
mvr <vlan-id>			Enters the MVR (Multicast VLAN Registration) configuration mode.	13
	exit		Exit from the MVR configuration mode.	13
	group <name-str> start-address <ip> end-address <ip>		Sets the multicast group range for the MVR.	13
	inactive		Disables MVR settings.	13
	mode <dynamic compatible>		Sets the MVR mode (dynamic or compatible).	13
	name <name-str>		Sets the MVR name for identification purposes.	13
	no	group	Disables all MVR group settings.	13
		group <name-str>	Disables the specified MVR group setting.	13
		inactive	Enables MVR.	13
		receiver-port <port-list>	Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
		source-port <port-list>	Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
		tagged <port-list>	Sets the port(s) to untag VLAN tags.	13
	receiver-port <port-list>		Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
	source-port <port-list>		Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
	tagged <port-list>		Sets the port(s) to tag VLAN tags.	13
	8021p-priority		Sets the 802.1p priority for the packets belonging to this VLAN group.	13

User and Enable Mode Commands

This chapter describes some commands which you can perform in the User and Enable modes.

46.1 Overview

The following command examples show how you can use User and Enable modes to diagnose and manage your Switch.

46.2 show Commands

These are the commonly used `show` commands.

46.2.1 show system-information

Syntax:

```
show system-information
```

This command shows the general system information (such as the firmware version and system up time).

An example is shown next.

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
sysname# show sys

System Name           : GS-4012F
System Contact        :
System Location       :
Ethernet Address      : 00:19:cb:00:00:02
ZyNOS F/W Version     : V3.80(TS.0)b5 | 04/13/2007
RomRasSize            : 3187522
System up Time        :      6:17:27 (228e9a ticks)
Bootbase Version      : V3.1 | 03/08/2007
ZyNOS CODE             : RAS Apr 12 2007 12:07:33
Product Model         : GS-4012F
sysname#
```

46.2.2 show ip

Syntax:

```
show ip
```

This command displays the IP related information (such as IP address and subnet mask) on all Switch interfaces.

The following figure shows the default interface settings.

```
sysname> show ip
Management IP Address
    IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
    IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
sysname>
```

46.2.3 show logging

Syntax:

```
show logging
```

This command displays the system logs. The following figure shows an example.

```
sysname# show logging
 1 Thu Jan  1 00:02:08 1970 PP05 -WARN  SNMP TRAP 3: link up
 2 Thu Jan  1 00:03:14 1970          INFO  adjtime task pause 1 day
 3 Thu Jan  1 00:03:16 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 4 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 1: warm start
 5 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 3: link up
 6 Thu Jan  1 00:03:16 1970 PINI  INFO  main: init completed
 7 Thu Jan  1 00:00:13 1970 PP26  INFO  adjtime task pause 1 day
 8 Thu Jan  1 00:00:14 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 9 Thu Jan  1 00:00:14 1970 PINI -WARN  SNMP TRAP 0: cold start
10 Thu Jan  1 00:00:14 1970 PINI  INFO  main: init completed
11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
Clear Error Log (y/n):
```



If you clear a log (by entering `y` at the `Clear Error Log (y/n):` prompt), you cannot view it again.

46.2.4 show interface

Syntax:

```
show interface [port-number]
```

This command displays statistics of a port. The following example shows that port 2 is up and the related information.

```
sysname# show interface 2
  Port Info      Port NO.      : 2
                  Link          : 100M/F
                  Status        : FORWARDING
                  LACP          : Disabled
                  TxPkts        : 0
                  RxPkts        : 63
                  Errors        : 0
                  Tx Kbs/s      : 0.0
                  Rx Kbs/s      : 0.0
                  Up Time       : 0:02:33
TX Packet      Tx Packets      : 0
                  Multicast     : 0
                  Broadcast     : 0
                  Pause         : 0
                  Tagged        : 0
RX Packet      Rx Packets      : 63
                  Multicast     : 0
                  Broadcast     : 63
                  Pause         : 0
                  Control       : 0
TX Collison    Single         : 0
                  Multiple     : 0
                  Excessive     : 0
                  Late          : 0
Error Packet   RX CRC         : 0
                  Length        : 0
                  Runt          : 0
Distribution   64             : 3
                  65 to 127     : 44
                  128 to 255    : 14
                  256 to 511    : 2
                  512 to 1023   : 0
                  1024 to 1518  : 0
                  Giant         : 0
sysname#
```

46.2.5 show mac address-table

Syntax:

```
show mac address-table <all <sort>|static>
```

Where

<sort> = Specifies the sorting criteria (MAC, VID or port).

This command displays the MAC address(es) stored in the Switch. The following example shows the static MAC address table.

```
sysname# show mac address-table static
Port      VLAN ID      MAC Address      Type
CPU       1          00:a0:c5:01:23:46 Static
sysname#
```

46.3 ping

Syntax:

```
ping <ip|host-name> < [in-band|out-of-band|vlan <vlan-id> ] [size
-> <0-1472>] [-t]>
```

where

<ip host-name>	=	The IP address or host name of an Ethernet device.
[in-band out-of-band vlan <vlan-id>]	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs. out-of-band refers to the management port while in-band means the other ports on the Switch.
[size <0-1472>]	=	Specifies the packet size to send.
[-t]	=	Sends Ping packets to the Ethernet device indefinitely. Press [CTRL]+ C to terminate the Ping process.

This command sends Ping packets to an Ethernet device. The following example sends Ping requests to and displays the replies from an Ethernet device with an IP address of 192.168.1.100.

sysname# ping 192.168.1.100								
sent	rcvd	rate	rtt	avg	mdev	max	min	reply from
1	1	100	0	0	0	0	0	192.168.1.100
2	2	100	0	0	0	0	0	192.168.1.100
3	3	100	0	0	0	0	0	192.168.1.100
sysname#								

46.4 traceroute

Syntax:

```
traceroute <ip|host-name> [in-band|out-of-band|vlan <vlan-id>][ttl
-> <1-255>] [wait <1-60>] [queries <1-10>]
```

where

<ip host-name>	=	The IP address or host name of an Ethernet device.
[in-band out-of-band vlan <vlan-id>]	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
[ttl <1-255>]	=	Specifies the Time To Live (TTL) period.
[wait <1-60>]	=	Specifies the time period to wait.
[queries <1-10>]	=	Specifies how many tries the Switch performs the traceroute function.

This command displays information about the route to an Ethernet device. The following example displays route information to an Ethernet device with an IP address of 192.168.1.100.

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
 1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
sysname>
```

46.5 Copy Port Attributes

Use the `copy running-config` command to copy attributes of one port to another port or ports.

Syntax:

```
copy running-config interface port-channel <port> <port-list>
copy running-config interface port-channel <port> <port-list>
-> [active] [name] [speed-duplex] [bpdu-control] [flow-control]
-> [intrusion-lock] [vlanlq] [vlanlq-member] [bandwidth-limit]
-> [vlan-stacking] [port-security] [broadcast-storm-control] [mirroring]
-> [port-access-authenticator] [queuing-method] [igmp-filtering]
-> [spanning-tree] [mrstp] [port-based-vlan] [mac-authentication] [trtcm]
-> [ethernet-oam] [loopguard] [arp-inspection] [dhcp-snooping]
```

where

copy running-config interface port-channel <port> <port-list>	= Copies all of the possible attributes from one port to another port or ports.
copy running-config interface port-channel <port> <port-list> [active...]	= Copies only the specified port attributes from one port to another port or ports.

An example is shown next.

- Copy all attributes of port 1 to port 2
- Copy selected attributes (active, bandwidth limit and STP settings) to ports 5-8

```
sysname# copy running-config interface port-channel 1 2
sysname# copy running-config interface port-channel 1 5-8 active
bandwidth-limit spanning-tree
```

46.6 Configuration File Maintenance

The following sections show how to manage the configuration files.

46.6.1 Using a Different Configuration File

You can store up to two configuration files on the Switch. Only one configuration file is used at a time. By default the Switch uses the first configuration file (with an index number of 1). You can set the Switch to use a different configuration file. There are two ways in which you can set the Switch to use a different configuration file: restart the Switch (cold reboot) and restart the system (warm reboot).

Use the `boot config` command to restart the Switch and use a different configuration file (if specified). The following example restarts the Switch to use the second configuration file.

```
sysname# boot config 2
```

Use the `reload config` command to restart the system and use a different configuration file (if specified). The following example restarts the system to use the second configuration file.

```
sysname# reload config 2
```



When you use the `write memory` command without specifying a configuration file index number, the Switch saves the changes to the configuration file the Switch is currently using.

46.6.2 Resetting to the Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 Enter `erase running config` to reset the current running configuration.
- 2 Enter `write memory` to save the changes to the current configuration file. If you want to reset the second configuration file, use the `write memory` command again with the specified index number.

The following example resets both configuration files to the factory default settings.

```
sysname# erase running-config
sysname# write memory
sysname# write memory 2
```

Configuration Mode Commands

This chapter describes how to enable and configure your Switch's features using commands. For more background information, see the feature specific chapters which proceed the commands chapters.

47.1 Change the Out of Band Management IP Address

Use the `ip address` command to change the IP address of the out of band management port on the Switch.

Syntax:

```
ip address <IP Address> <Subnet Mask>
```

An example is shown next.

- Change the out of band Management IP address to 192.168.0.2
- View updated settings.

```
sysname(config)# ip address 192.168.0.2 255.255.255.0
sysname(config)# exit
sysname# show ip
Management IP Address
    IP[192.168.0.2], Netmask[255.255.255.0], VID[0]
IP Interface
    IP[192.168.2.1], Netmask[255.255.255.0], VID[2]
```

See example in [Section 48.2 on page 395](#) for information on how to change the in band management IP address for the Switch.

47.2 Enabling IGMP Snooping

To enable IGMP snooping on the Switch. Enter `igmp-snooping` and press [ENTER]. You can also set how to treat traffic from an unknown multicast group by typing the `unknown-multicast-frame` parameter.

Syntax:

```
igmp-snooping
igmp-snooping 8021p-priority <0-7>
igmp-snooping host-timeout <1-16711450>
igmp-snooping leave-timeout <1-16711450>
igmp-snooping unknown-multicast-frame <drop|flooding>
igmp-snooping reserved-multicast-group <drop|flooding>
```

where

<code>igmp-snooping</code>	=	Enables IGMP snooping on the Switch.
<code>8021p-priority</code>	=	Sets a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets.
<code>host-timeout <1-16711450></code>	=	Specifies the time out period of the Switch with respect to IGMP report queries. If an IGMP report for a multicast group was not received for a host-timeout period, from a specific port, this port is deleted from the member list of that multicast group.
<code>leave-timeout <1-16711450></code>	=	Specifies the time that the Switch will wait for multicast members to respond to a leave report. If no response happens in the timeout period, the Switch deletes the port from the multicast group.
<code>unknown-multicast-frame <drop flooding></code>	=	Specifies whether you want to discard packets from unknown multicast groups or whether you want to forward them to all ports.
<code>reserved-multicast-group <drop flooding></code>	=	Specifies whether you want to discard packets in the reserved multicast groups or whether you want to forward them to all ports.

An example is shown next.

- Enable IGMP snooping on the Switch.
- Set the `host-timeout` and `leave-timeout` values to 30 seconds
- Set the Switch to drop packets from unknown multicast groups.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping leave-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop
```

47.3 Configure IGMP Filter

Use the following commands in the config mode to configure IGMP filtering profiles.

Syntax:

```
igmp-filtering
igmp-filtering profile <name> start-address <ip> end-address <ip>
```

where

<code>igmp filtering</code>	=	Enables IGMP filtering on the Switch
<code>profile <name></code>	=	Specifies a name (up to 32 alphanumeric characters) for this IGMP profile. If you want to edit an existing IGMP profile enter the existing profile name followed by <code>start-address</code> and <code>end-address</code> parameters.
<code>start-address</code>	=	Specifies the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.
<code>end-address</code>	=	Specifies the ending multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.

An example is shown next.

- Enable IGMP filtering on the Switch.
- Create an IGMP filtering profile **filter1** and specify the multicast IP addresses in the range **224.255.255.0** to **225.255.255.255** to belong to this profile.

```
sysname(config)# igmp-filtering
sysname(config)# igmp-filtering profile filter1 start-address
224.255.255.0 end-address 225.255.255.255
```

47.4 Enabling STP

Use the `spanning-tree` or the `mrstp` commands to enable and configure STP on the Switch. The difference between the commands is that `spanning-tree` only allows you to set up one spanning tree configuration and the `mrstp` command allows you to set up multiple ones.

Syntax:

```
spanning-tree
spanning-tree priority <0-61440>
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>
spanning-tree <port-list> path-cost <1-65535>
spanning-tree <port-list> priority <0-255>
```

and

```
mrstp <treeIndex> <cr>
mrstp <treeIndex> priority <0-61440>
mrstp <treeIndex> hello-time <1-10> maximum-age <6-40> forward-delay
-> <4-30>
mrstp interface <port-list> <cr>
mrstp interface <port-list> path-cost <1-65535>
mrstp interface <port-list> priority <0-255>
mrstp interface <port-list> treeIndex <1-4>
```

where

<code>spanning-tree</code>	=	Enables STP on the Switch.
<code>mrstp <treeIndex></code>		Enables a specific tree configuration.
<code>priority <0-61440></code>	=	<p>Specifies the bridge priority for the Switch. The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Bridge priority is used in determining the root switch, root port and designated port. The Switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>
<code>hello-time <1-10></code>	=	Specifies the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
<code>maximum-age <6-40></code>	=	Specifies the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network.
<code>forward-delay <4-30></code>	=	Specifies the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
<code><port-list> path-cost <1-65535></code>	=	<p>Enables STP on the specified ports.</p> <p>Specifies the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge.</p>
<code><port-list> priority <0-255></code>	=	<p>Specifies the priority for each port.</p> <p>Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first.</p>
<code><port-list> treeIndex <1-4></code>	=	Specifies which STP configuration these ports will participate in. (mrstp command only).

An example using `spanning-tree` command is shown next.

- Enable STP on the Switch.
- Set the bridge priority of the Switch to 0.
- Set the Hello Time to 4, Maximum Age to 20 and Forward Delay to 15 on the Switch.

- Enable STP on port 5 with a path cost of 150.
- Set the priority for port 5 to 20.

```
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay
15
sysname(config)# spanning-tree 5 path-cost 150
sysname(config)# spanning-tree 5 priority 20
```

47.5 no Command Examples

These are the commonly used command examples that belong to the `no` group of commands. The `no` group commands are commands which are preceded by keyword `no`. This command negates the intended action of the command. In most cases the `no` command disables, resets or clears settings. There are cases, however, where the `no` command can activate features. This section shows some uses of these commands.

47.5.1 Disable Commands

Use the `no` command to disable features on the Switch.

Syntax:

```
no spanning-tree
no mirror-port
```

Disables STP on the Switch.

Disables port mirroring on the Switch.

47.5.2 Resetting Commands

Use the `no` command to reset Switch settings to their default values.

Syntax:

```
no https timeout
```

Resets the https session timeout to default.

An example is shown next. The session timeout is reset to 300 seconds.

```
sysname(config)# no https timeout
Cache timeout 300
```

47.5.3 Re-enable commands

The `no` command can also be used to re-enable features which have been disabled.

Syntax:

```
no ip route <ip> <mask> inactive
```

where

<ip> <mask> inactive = Re-enables an ip route with the specified IP address and subnet mask.

An example is shown next.

- Enable the IP route with the IP address of 192.168.11.1 and subnet mask of 255.255.255.0. This ip route must have already been created and made inactive prior to re-enable command being applied.

```
sysname(config)# no ip route 192.168.11.1 255.255.255.0 inactive
```

47.5.4 Other Examples of no Commands

In some cases the `no` command can disable a feature, disable an option of a feature or disable a feature on a port by port basis.

47.5.4.1 no trunk

Syntax:

```
no trunk <T1|T2|T3|T4|T5|T6>
no trunk <T1|T2|T3|T4|T5|T6> lacp
no trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
```

where

<T1|T2|T3|T4|T5|T6> = Disables the trunk group.
<T1|T2|T3|T4|T5|T6> = Disables LACP in the trunk group.
lacp
<T1|T2|T3|T4|T5|T6> = Removes ports from the trunk group.
interface <port-list>

An example is shown next.

- Disable trunk one (T1).
- Disable LACP on trunk three (T3).
- Remove ports one, three, four and five from trunk two (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T2 interface 1,3-5
```

47.5.4.2 no port-access-authenticator

Syntax:

```
no port-access-authenticator
no port-access-authenticator <port-list> reauthenticate
no port-access-authenticator <port-list>
```


where

	=	Disables port authentication on the Switch.
<port-list> reauthenticate	=	Disables the re-authentication mechanism on the listed port(s).
<port-list>	=	Disables authentication on the listed ports.

An example is shown next.

- Disable authentication on the Switch.
- Disable re-authentication on ports one, three, four and five.
- Disable authentication on ports one, six and seven.

Figure 203 no port-access-authenticator Command Example

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

47.5.4.3 no ssh

Syntax:

```
no ssh key <rsal|rsa|dsa>
no ssh known-hosts <host-ip>
no ssh known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]
```

where

key <rsal rsa dsa>	=	Disables the secure shell server encryption key. Your Switch supports SSH versions 1 and 2 using RSA and DSA authentication.
known-hosts <host-ip>	=	Removes a specific remote host from the list of all known hosts.
known-hosts <host-ip> [1024 ssh-rsa ssh-dsa]	=	Removes remote known hosts with a specified public key type (1024-bit RSA1, RSA or DSA).

An example is shown next.

- Disable the secure shell RSA1 encryption key.
- Remove the remote host with IP address 172.165.1.8 from the list of known hosts.
- Remove the remote host with IP address 172.165.1.9 and with an SSH-RSA encryption key from the list of known hosts.

```
sysname(config)# no ssh key rsal
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

47.6 Static Route Commands

You can create and configure static routes on the Switch by using the `ip route` command.

Syntax:

```
ip route <ip> <mask> <next-hop-ip>
ip route <ip> <mask> <next-hop-ip> [metric <metric>][name <name>]
--> [inactive]
```

where

<code><ip></code>	=	Specifies the network IP address of the final destination.
<code><mask></code>	=	Specifies the subnet mask of this destination.
<code><next-hop-ip></code>	=	Specifies the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
<code>[metric <metric>]</code>	=	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
<code>[name <name>]</code>	=	Specifies a descriptive name (up to 32 printable ASCII characters) for identification purposes.
<code>[inactive]</code>	=	Deactivates a static route

An example is shown next.

- Create a static route with the destination IP address of 172.21.1.104, subnet mask of 255.255.0.0 and the gateway IP address of 192.168.1.2.
- Assigns a metric value of 2 to the static route.
- Assigns the name “route1” to the static route.

```
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 metric 2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 name route1
```

47.7 Enabling MAC Filtering

You can create a filter to drop packets based on the MAC address of the source or the destination.

Syntax:

```
mac-filter name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>
```

where

<code>name <name></code>	=	Names the filtering rule.
<code>mac <mac-addr></code>	=	Specifies the MAC address you want to filter.
<code>vlan <vlan-id></code>	=	Specifies which VLAN this rule applies to.
<code>drop <src/dst/both></code>	=	Selects the behavior of the rule. <ul style="list-style-type: none"> • <code>src</code> - drop packets coming from the specified MAC address • <code>dst</code> - drop packets going to the specified MAC address • <code>both</code> - drop packets coming from or going to the specified MAC address

An example is shown next.

- Create a filtering rule called “filter1”.
- Drop packets coming from and going to MAC address 00:12:00:12:00:12 on VLAN.

```
sysname(config)# mac-filter name filter 1
sysname(config)# mac-filter name filter 1 mac 00:12:00:12:00:12 vlan 1 drop
both
```

47.8 Enabling Trunking

To create and enable a trunk, enter `trunk` followed by the ports which you want to group and press [ENTER].

Syntax:

```
trunk <T1|T2|T3|T4|T5|T6>
trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
trunk <T1|T2|T3|T4|T5|T6> lacp
```

where

<code><T1 T2 T3 T4 T5 T6></code>	=	Enables the trunk.
<code><T1 T2 T3 T4 T5 T6></code> <code>interface <port-list></code>	=	Places ports in the trunk.
<code><T1 T2 T3 T4 T5 T6> lacp</code>	=	Enables LACP in the trunk.

An example is shown next.

- Create trunk 1 on the Switch.
- Place ports 5-8 in trunk 1.

- Enable dynamic link aggregation (LACP) on trunk 1.

```
sysname(config)# trunk t1
sysname(config)# trunk t1 interface 5-8
sysname(config)# trunk t1 lacp
```

47.9 Enabling Port Authentication

To enable a port authentication, you need to specify your RADIUS server details and select the ports which require external authentication. You can set up multiple RADIUS servers and specify how the Switch will process authentication requests.

47.9.1 RADIUS Server Settings

Configuring multiple RADIUS servers is only available via the command interpreter mode. Use the `radius-server` command to set up your RADIUS server settings.

Syntax:

```
radius-server host <index> <ip>
radius-server host <index> <ip> [acct-port <socket-number>] [key
--> <key-string>]
radius-server timeout <1-1000>
radius-server mode <priority|round-robin>
```

where

<code>radius-server host <index></code>	=	Specifies the IP address of the RADIUS server.
<code><ip></code>		
<code>[acct-port <socket-number>]</code>	=	Changes the UDP port of the RADIUS server from the default (1812).
<code>[key <key-string>]</code>	=	Specifies a password (up to 32 alphanumeric characters) as the key to be shared between the RADIUS server and the Switch.

<code>radius-server timeout <1-1000></code>	=	Specifies the timeout period (in seconds) the Switch will wait for a response from a RADIUS server. If 2 RADIUS servers are configured, this is the total time the Switch will wait for a response from either server.
<code>mode <priority round-robin></code>	=	Specifies the way the Switch will process requests from the clients to the RADIUS server. (Only applicable with multiple RADIUS servers configured.)
<code>priority</code>	-	When a client sends an authentication request through the Switch to the RADIUS server. The Switch will forward the request to the RADIUS server. If no response within half the timeout period, it will forward the request to the second RADIUS server.
<code>round-robin</code>	-	When a client sends an authentication request through the Switch to the RADIUS server. The Switch will forward the request to the first RADIUS server. If there is no response within the timeout period, the request times out. The client sends an authentication request again and the Switch forwards the request to the second RADIUS server.

See [Section 47.9.2 on page 393](#) for an example.

47.9.2 Port Authentication Settings

Use the `port-access-authenticator` command to configure port security on the Switch.

Syntax:

```
port-access-authenticator
port-access-authenticator <port-list>
port-access-authenticator <port-list> reauthenticate
port-access-authenticator <port-list> reauth-period <reauth-period>
```

where

<code>port-access-authenticator</code>	=	Enables port authentication on the Switch.
<code>port-access-authenticator <port-list></code>	=	Specifies which ports require authentication.
<code>reauthenticate</code>	=	Enables reauthentication on the port.
<code>reauth-period <reauth-period></code>	=	Specifies how often a client has to re-enter his or her username and password to stay connected to the port.

An example is shown next.

- Specify RADIUS server 1 with IP address 10.10.10.1, port 1890 and the string secretKey as the password. See [Section 47.9.1 on page 392](#) for more information on RADIUS server commands.
- Specify the timeout period of 30 seconds that the Switch will wait for a response from the RADIUS server.
- Enable port authentication on ports 4 to 8.
- Activate reauthentication on the ports.
- Specify 1800 seconds as the interval for client reauthentication.

```
sysname(config)# radius-server host 1 10.10.10.1 acct-port 1890 key  
--> secretKey  
sysname(config)# radius-server timeout 30  
sysname(config)# port-access-authenticator  
sysname(config)# port-access-authenticator 4-8  
sysname(config)# port-access-authenticator 4-8 reauthenticate  
sysname(config)# port-access-authenticator 4-8 reauth-period 1800
```

Interface Commands

These are some commonly used configuration commands that belong to the interface group of commands.

48.1 Overview

The interface commands allow you to configure the Switch on a port by port basis.

48.2 Interface Command Examples

This section provides examples of some frequently used interface commands.

48.2.1 interface port-channel

Use this command to enable the specified ports for configuration. Indicate multiple, non-sequential ports separated by a comma. Use a dash to specify a port range.

Syntax:

```
interface port-channel <port-list>
```

An example is shown next.

- Enter the configuration mode.
- Enable ports 1, 3, 4 and 5 for configuration.
- Begin configuring for those ports.

```
sysname# config
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)#
```

48.2.2 bpdu-control

Syntax:

```
bpdu-control <peer|tunnel|discard|network>
```

where

<code><peer tunnel discard network></code>	=	Type <code>peer</code> to process any BPDUs received on these ports. Type <code>tunnel</code> to forward BPDUs received on these ports. Type <code>discard</code> to drop any BPDUs received on these ports. Type <code>network</code> to process a BPDU with no VLAN tag and forward a tagged BPDU.
---	---	--

An example is shown next.

- Enable ports 1, 3, 4 and 5 for configuration.
- Set the BPDU control to `tunnel`, to forward BPDUs received on ports one, three, four and five.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# bpdu-control tunnel
sysname(config-interface)#
```

48.2.3 broadcast-limit

Syntax:

```
broadcast-limit
broadcast-limit <pkt/s>
```

where

<code>broadcast-limit</code>	=	Enables broadcast storm control limit on the Switch.
<code><pkt/s></code>	=	Limits how many broadcast packet the interface receives per second.

An example is shown next.

- Enable port one for configuration.
- Enable broadcast control.
- Set how many broadband packets the interface receives per second.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 21
```

48.2.4 bandwidth-limit

The `bandwidth-limit` command enables bandwidth control on the Switch.

Syntax:

```
bandwidth-limit
bandwidth-limit pir <Kbps>
bandwidth-limit cir <Kbps>
bandwidth-limit egress <Kbps>
```


where

<code>pir <Kbps></code>	=	Sets the maximum bandwidth allowed for incoming traffic.
<code>cir <Kbps></code>	=	Sets the guaranteed bandwidth allowed for incoming traffic.
<code>egress <Kbps></code>	=	Sets the maximum bandwidth allowed for outgoing traffic (egress) on the Switch.

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the outgoing traffic bandwidth limit to 5000Kbps.
- Set the guaranteed bandwidth allowed for incoming traffic to 4000Kbps.
- Set the maximum bandwidth allowed for incoming traffic to 8000Kbps.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit
sysname(config-interface)# bandwidth-limit egress 5000
sysname(config-interface)# bandwidth-limit cir 4000
sysname(config-interface)# bandwidth-limit pir 8000
```

48.2.5 mirror

The `mirror` command enables port mirroring on the interface.

Syntax:

```
mirror
mirror dir <ingress|egress|both>
```

where

<code>dir</code> <code><ingress egress both></code>	=	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.
--	---	--

Port mirroring copies traffic from one or all ports to another or all ports for external analysis.

An example is shown next.

- Enable port mirroring.
- Enable the monitor port 3.
- Enable ports 1, 4, 5 and 6 for configuration.
- Enable port mirroring on the ports.

- Enable port mirroring for outgoing traffic. Traffic is copied from ports 1, 4, 5 and 6 to port three in order to examine it in more detail without interfering with the traffic flow on the original ports.

```
sysname(config)# mirror-port  
sysname(config)# mirror-port 3  
sysname(config)# interface port-channel 1,4-6  
sysname(config-interface)# mirror  
sysname(config-interface)# mirror dir egress
```

48.2.6 gvrp

Syntax:

gvrp

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

An example is shown next.

- Enable the IEEE 802.1Q tagged VLAN command to configure tagged VLAN for the Switch.
- Enable ports one, three, four and five for configuration.
- Enable GVRP on the interface.

```
sysname(config)# vlan1q gvrp  
sysname(config)# interface port-channel 1,3-5  
sysname(config-interface)# gvrp
```

48.2.7 ingress-check

The `ingress-check` command enables the device to discard incoming frames for VLANs that do not have this port as a member.

Syntax:

ingress-check

An example is shown next.

- Enable ports 1, 3, 4 and 5 for configuration.
- Enable ingress checking on the interface.

```
sysname(config)# interface port-channel 1,3-5  
sysname(config-interface)# ingress-check
```

48.2.8 frame-type

Syntax:

frame-type <all|tagged|untagged>

where

`<all|tagged|untagged>` = Choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable ingress checking on the ports.
- Enable tagged frame-types on the interface.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
sysname(config-interface)# frame-type tagged
```

48.2.9 weight

Syntax:

`weight <wt1> <wt2> ... <wt8>`

where

`<wt1> <wt2> ... <wt8>` = Sets the interface WFQ weighting. A weight value of one to eight is given to each variable from `wt 1` to `wt 8`.

An example is shown next.

- Enable WRR queuing on ports 2 and 6 to 8.
- Enable port 2 and ports 6 to 8 for configuration.
- Set the queue weights from Q0 to Q7.

```
sysname# configure
sysname(config)# interface port-channel 2,6-8
sysname(config-interface)# wrr
sysname(config-interface)# weight 8 7 6 5 4 3 2 1
```

48.2.10 egress set

Syntax:

`egress set <port-list>`

where

`<port-list>` = Sets the outgoing traffic port list for a port-based VLAN.

An example is shown next.

- Enable port-based VLAN tagging on the Switch.
- Enable ports one, three, four and five for configuration.

- Set the outgoing traffic ports as the CPU (0), seven (7) and eight (8).

```
sysname(config)# vlan-type port-based
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# egress set 0,7,8
```

48.2.11 qos priority

Syntax:

```
qos priority <0 .. 7>
```

where

`<0 .. 7>` = Sets the quality of service priority for a port.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the IEEE 802.1p quality of service priority as four (4).

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
```

48.2.12 name

Syntax:

```
name <port-name-string>
```

where

`<port-name-string>` = Sets a name for your port interface.

An example is shown next.

- Enable port one for configuration.
- Set a name for the port.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# name Test
```

48.2.13 speed-duplex

Syntax:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

where

<pre><auto 10-half 10- full 100-half 100- full 1000-full></pre>	<p>= Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the port. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.</p>
---	--

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the speed to 100 Mbps in half duplex mode.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# speed-duplex 100-half
```

48.2.14 test

You can perform an interface loopback test on specified ports. The test returns `Passed!` or `Failed!`

An example is shown next.

- Select ports 3-6 for internal loopback test.
- Execute the test command.
- View the results.

```
sysname(config)# interface port-channel 3-6
sysname(config-interface)# test 3-6
Testing internal loopback on port 3 :Passed!
  Ethernet Port 3 Test ok.
Testing internal loopback on port 4 :Passed!
  Ethernet Port 4 Test ok.
Testing internal loopback on port 5 :Passed!
  Ethernet Port 5 Test ok.
Testing internal loopback on port 6 :Passed!
  Ethernet Port 6 Test ok.
```

48.3 Interface no Command Examples

Similar to the no commands in the Enable and Config modes, the no commands for the Interface sub mode also disable certain features. In this mode, however, this takes place on a port by port basis.

48.3.1 no bandwidth-limit

You can disable bandwidth limit on port 1 simply by placing the `no` command in front of the `bandwidth-limit` command.

Syntax:

```
no bandwidth-limit
```

An example is shown next:

- Disable bandwidth limit on port1

```
sysname(config)# interface port-channel 1  
sysname(config-interface)# no bandwidth-limit
```

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

49.1 Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

- 1 Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the Switch.
 - Use the `vlan <vlan-id>` command to configure or create a VLAN on the Switch. The Switch automatically enters the `config-vlan` mode. Use the `inactive` command to deactivate the VLAN(s).
 - Use the `interface port-channel <port-list>` command to enter the `config-interface` mode to set the VLAN settings on a port, then use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list to that specific port in the PVID table.
 - Use the `exit` command when you are finished configuring the VLAN.

```
sysname (config)# vlan 2000
sysname (config-vlan)# name upl
sysname (config-vlan)# fixed 5-8
sysname (config-vlan)# no untagged 5-8
sysname (config-vlan)# exit
sysname (config)# interface port-channel 5-8
sysname (config-interface)# pvid 2000
sysname (config-interface)# exit
```

- 2 Configure your management VLAN.
 - Use the `vlan <vlan-id>` command to create a VLAN (VID 3 in this example) for managing the Switch, and the Switch will activate the new management VLAN.
 - Use the `inactive` command to disable the new management VLAN.

```
sysname (config)# vlan 3
sysname (config-vlan)# inactive
```

49.2 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

49.2.1 GARP Status

Syntax:

```
show garp
```

This command shows the Switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
sysname# show garp
GARP Timer
-----
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
sysname#
```

49.2.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

- | | | |
|--------------------|---|---|
| join <msec> | = | This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds. |
| leave <msec> | = | This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds. |
| leaveall
<msec> | = | This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds. |

This command sets the Switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
sysname (config)# garp join 300 leave 800 leaveall 11000
```

49.2.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the Switch's GVRP settings.

An example is shown next.

```
sysname# show vlan1q gvrp
GVRP Support
-----
gvrpEnable = YES
sysname #
```

49.2.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the Switch.

49.2.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the Switch does not propagate VLAN information to other switches.

49.3 Port VLAN Commands

You must configure the Switch port VLAN settings in config-interface mode.

49.3.1 Set Port VID

Syntax:

```
pvid <VID>
```

where

<VID> = Specifies the VLAN number between 1 and 4094.

This command sets the default VLAN ID on the port(s).

The following example sets the default VID to 200 on ports 1 to 5.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# pvid 200
```

49.3.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

<code><all tagged untagged></code>	=	Specifies all Ethernet frames (tagged and untagged), only tagged Ethernet frames or only untagged Ethernet frames.
--	---	--

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# frame-type tagged
```

49.3.3 Enable or Disable Port GVRP

Use the `gvrp` command to enable GVRP on the port(s). Use the `no gvrp` command to disable GVRP.

The following example turns off GVRP for ports 1 to 5.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# no gvrp
```

49.3.4 Modify Static VLAN

Use the following commands in the `config-vlan` mode to configure the static VLAN table.

Syntax:

```
vlan <vlan-id>
fixed <port-list>
forbidden <port-list>
name <name-str>
normal <port-list>
untagged <port-list>
no fixed <port-list>
no forbidden <port-list>
no untagged <port-list>
```

where

<vlan-id> = The VLAN ID [1 – 4094].
 <name-str> = A name to identify the SVLAN entry.
 <port-list> = This is the Switch port list.

- Enter `fixed` to register the <port-list> to the static VLAN table with <vlan-id>.
- Enter `normal` to confirm registration of the <port-list> to the static VLAN table with <vlan-id>.
- Enter `forbidden` to block a <port-list> from joining the static VLAN table with <vlan-id>.
- Enter `no fixed` or `no forbidden` to change <port-list> to normal status.
- Enter `untagged` to send outgoing frames without a tag.
- Enter `no untagged` to tag outgoing frames.

49.3.4.1 Modify a Static VLAN Table Example

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

```
sysname (config)# vlan 2000
sysname (config-vlan)# fixed 1-5
sysname (config-vlan)# untagged 1-5
```

49.3.4.2 Forwarding Process Example

49.3.4.2.1 Tagged Frames

- 1 First the Switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
- 2 The Switch then checks the VID in a frame's tag against the SVLAN table.
- 3 The Switch notes what the SVLAN table says (that is, the SVLAN tells the Switch whether or not to forward a frame and if the forwarded frames should have tags).
- 4 Then the Switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

49.3.4.2.2 Untagged Frames

- 1 An untagged frame comes in from the LAN.
- 2 The Switch checks the PVID table and assigns a temporary VID of 1.
- 3 The Switch ignores the port from which the frame came, because the Switch does not send a frame to the port from which it came. The Switch also does not forward frames to "forbidden" ports.
- 4 If after looking at the SVLAN, the Switch does not have any ports to which it will send the frame, it won't check the port filter.

49.3.5 Delete VLAN ID

Syntax:

```
no vlan <vlan-id>
```

where

`<vlan-id>` = The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

```
sysname (config)# no vlan 2
```

49.4 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

49.5 Disable VLAN

Syntax:

```
vlan <vlan-id> inactive
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

49.6 Show VLAN Setting

Syntax:

```
show vlan
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

- VID is the VLAN identification number.
- Status shows whether the VLAN is static or active.
- Elap-Time is the time since the VLAN was created on the Switch.

- The TagCtl section of the last column shows which ports are tagged and which are untagged.

```
sysname# show vlan
The Number of VLAN:    3
Idx. VID  Status      Elap-Time      TagCtl
-----
1    1    Static      0:12:13      Untagged :1-2
                        Tagged   :
1   100    Static      0:00:17      Untagged :
                        Tagged   :1-4
1   200    Static      0:00:07      Untagged :1-2
                        Tagged   :3-8
```


Multicast VLAN Registration Commands

This chapter shows you how to use Multicast VLAN Registration (mvr) commands.

50.1 Overview

Use the mvr commands in the configuration mode to create and configure multicast VLANs.



If you want to enable IGMP snooping see [Section 47.2 on page 383](#).

50.2 Create Multicast VLAN

Use the following commands in the config-mvr mode to configure a multicast VLAN group.

Syntax:

```
mvr <vlan-id>
mvr <vlan-id> source-port <port-list>
mvr <vlan-id> receiver-port <port-list>
mvr <vlan-id> inactive
mvr <vlan-id> mode <dynamic|compatible>
mvr <vlan-id> name <name-str>
mvr <vlan-id> tagged <port-list>
mvr <vlan-id> group <name-str> start-address <ip> end-address <ip>
mvr <vlan-id> exit
```

where

<code><vlan-id></code>	=	The VLAN ID [1 – 4094].
<code>source-port <port-list></code>	=	Specifies the MVR source ports which send and receive multicast traffic.
<code>receiver-port <port-list></code>	=	Specifies the MVR receiving ports which only receive multicast traffic.
<code>name <name-str></code>	=	A name to identify the multicast VLAN group.

mode <dynamic compatible>	=	Specifies dynamic (sends IGMP reports to all source ports in the multicast VLAN) or compatible (does not send IGMP reports).
group name <name-str>	=	A name to identify the MVR IP multicast group.
start-address <ip>	=	Specifies the starting IP multicast address of the multicast group in dotted decimal notation.
end-address <ip>	=	Specifies the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the start-address if you want to configure only one IP address for the multicast group.

- Enter MVR mode. Create a multicast VLAN with the name `multivlan` and the VLAN ID of 3.
- Specify source ports 2, 3, 5 and receiver ports 6-8.
- Specify dynamic mode for the multicast group.
- Configure MVR multicast group addresses by the name of `ipgroup`.
- Exit MVR mode.

See the following example.

```
sysname(config)# mvr 3
sysname(config-mvr)# name multivlan
sysname(config-mvr)# source-port 2,3,5
sysname(config-mvr)# receiver-port 6-8
sysname(config-mvr)# mode dynamic
sysname(config-mvr)# group ipgroup start-address 224.0.0.1 end-address
--> 224.0.0.255
sysname(config-mvr)# exit
```


Routing Domain Command Examples

51.0.1 interface route-domain

Syntax:

```
interface route-domain <ip-address>/<mask-bits>
```

where

- <ip-address> = This is the IP address of the Switch in the routing domain. Specify the IP address is dotted decimal notation. For example, 192.168.1.1.
- <mask-bits> = The number of bits in the subnet mask. Enter the subnet mask number preceded with a “/”. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24).

Use this command to enable/create the specified routing domain for configuration.

An example is shown next.

- Enter the configuration mode.
- Enable default routing domain (the 192.168.1.1 subnet) for configuration.
- Begin configuring for this domain.

```
sysname# config
sysname(config)# interface route-domain 192.168.1.1/24
cmd interface route domain
192.168.1.1 255.255.255.0
sysname(config-if)#
```


Troubleshooting

This chapter covers potential problems and possible remedies.

52.1 Problems Starting Up the Switch

Table 144 Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the Switch.	Check the power connection and make sure the power source is turned on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

52.2 Problems Accessing the Switch

Table 145 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the Switch using Telnet.	<p>Make sure the ports are properly connected.</p> <p>You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.</p> <p>Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.</p>
I cannot access the web configurator.	<p>The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.</p> <p>If you have configured more than one IP interface, make sure another administrator is NOT logged into the web configurator on a different IP interface using the same account.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.</p> <p>Your computer's and the Switch's IP addresses must be on the same subnet.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>

52.2.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).



Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

52.2.1.1 Internet Explorer Pop-up Blockers

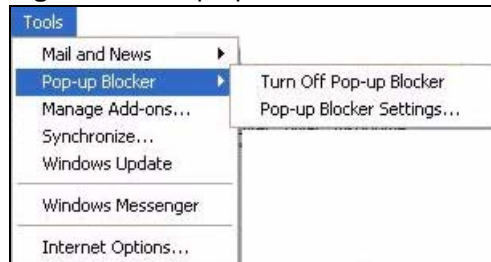
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

52.2.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 204 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

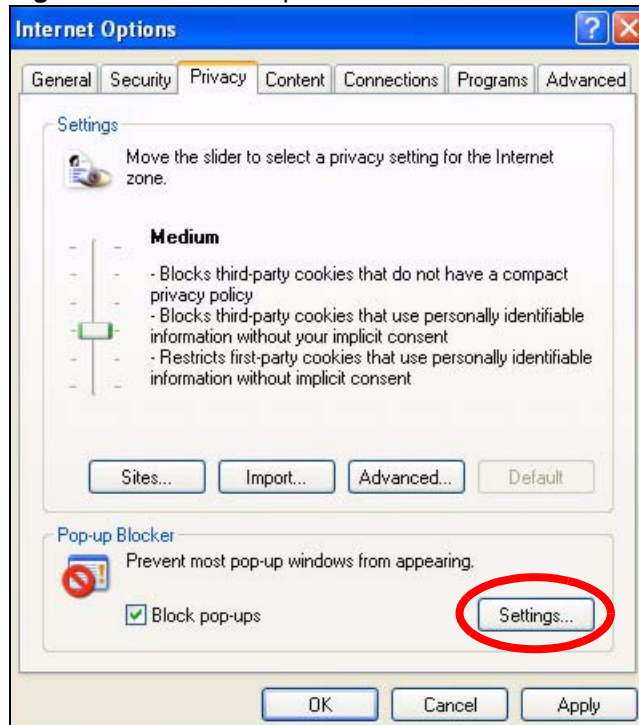
Figure 205 Internet Options

3 Click **Apply** to save this setting.

52.2.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1** In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2** Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 206 Internet Options

- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 207 Pop-up Blocker Settings

- 5 Click **Close** to return to the **Privacy** screen.

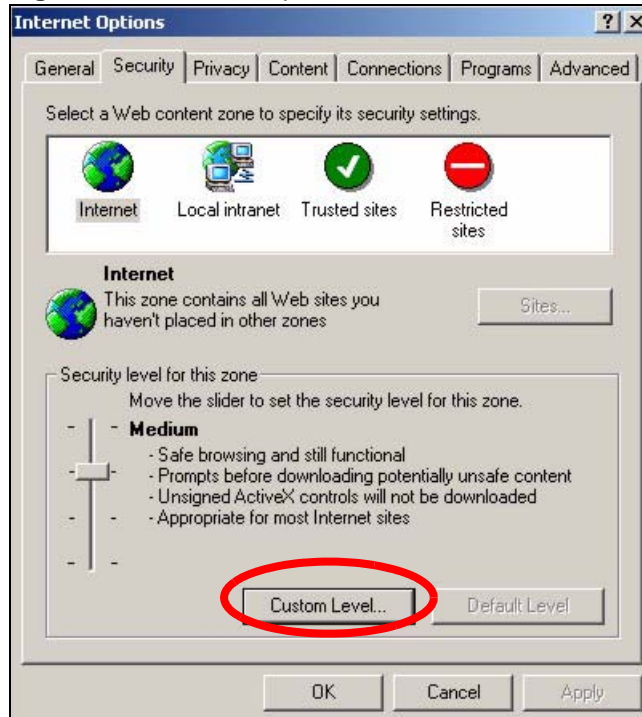
- 6 Click **Apply** to save this setting.

52.2.1.2 JavaScripts

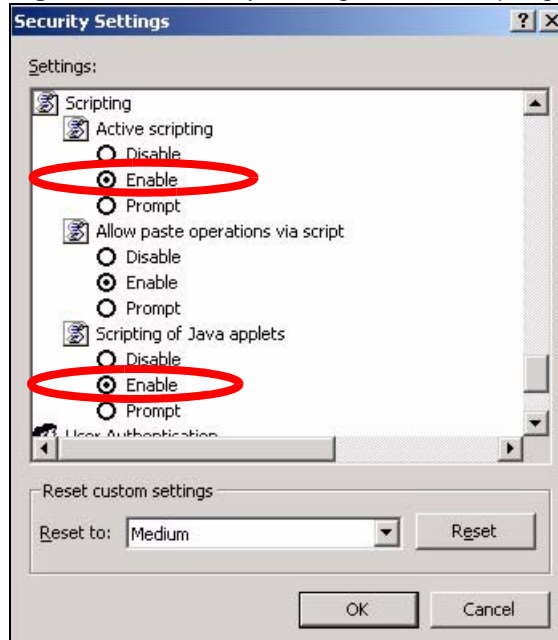
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

Figure 208 Internet Options

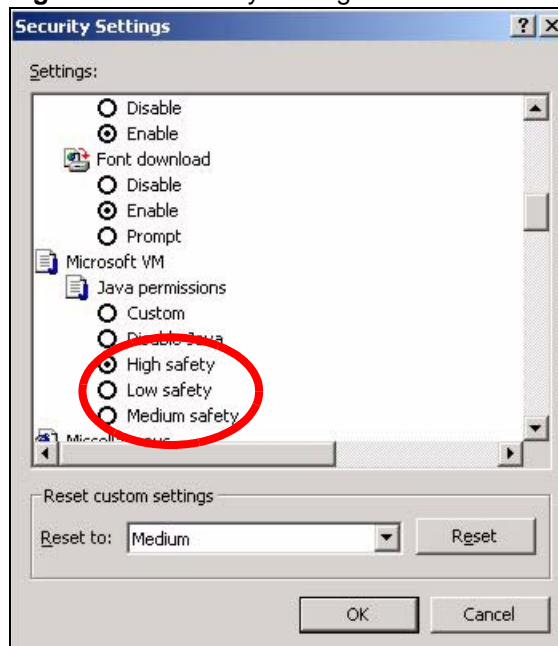


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 209 Security Settings - Java Scripting

52.2.1.3 Java Permissions

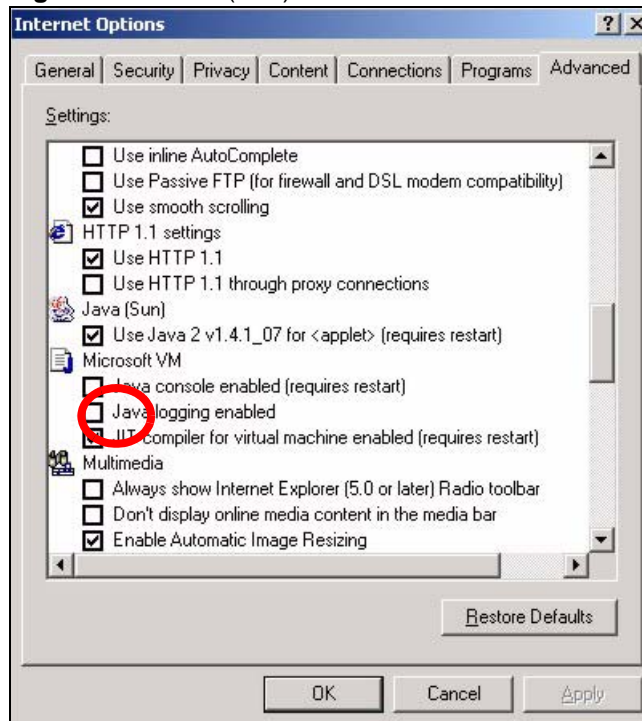
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 210 Security Settings - Java

52.2.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 211 Java (Sun)



52.3 Problems with the Password

Table 146 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.

PART VI

Appendices and Index

Product Specifications (425)
IP Addresses and Subnetting (431)
Common Services (441)
Legal Information (445)
Customer Support (449)
Index (453)

Product Specifications

The following tables summarize the Switch's hardware and firmware features.

Table 147 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	Standard 19" rack mountable GS-4012F : 438 mm (W) x 225 mm (D) x 44.45 mm (H) GS-4024 : 438 mm (W) x 300 mm (D) x 44.45 mm (H)
Weight	GS-4012F : 3.1 Kg GS-4024 : 4.2 Kg
Power Specification	One Backup Power Supply (BPS) connector GS-4012F AC: 100-240 VAC 50/60 Hz, 1.5 A Max. DC: -48 VDC ~ -60 VDC, 1.6 A Max. GS-4024 AC: 100-240 VAC 50/60 Hz 1.5 A Max. DC: -48 VDC ~ -60 VDC, 2.2 A Max. Note: There is no tolerance for the DC input voltage
Interfaces	GS-4012F : 8 mini-GBIC (SFP) slots GS-4024 : 20 10/100/1000 Base-Tx ports All Models: 4 GbE Dual Personality interfaces (Each interface has one 1000Base-T copper port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.) One local management Ethernet port Auto-negotiation Auto-MDIX One console port Compliant with IEEE 802.3ad/u/x Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Per switch: BPS, PWR, SYS, ALM Per Gigabit Ethernet/mini-GBIC port: 100, 1000/LNK, ACT Per mini-GBIC port: LNK, ACT Per Management port: 10, 100
Operating Environment	Temperature: 0° C ~ 45° C (32° F ~ 113° F) Humidity: 10 ~ 90% (non-condensing)
Storage Environment	Temperature: -10° C ~ 70° C (13° F ~ 158° F) Humidity: 10 ~ 90% (non-condensing)
Ground Wire Gauge	18 AWG or larger

Table 147 Hardware Specifications

Power Wire Gauge	18 AWG or larger
Fuse Specification	250 VAC, T2A

Table 148 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	In band: 192.168.1.1 Out of band (Management port): 192.168.0.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
IP Routing Domain	An IP interface (also known as an IP routing domain) is not bound to a physical port. Configure an IP routing domain to allow the Switch to route traffic between different networks.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Switch assign IP addresses, an IP default gateway and DNS servers to computers on your network.
IGMP Snooping	The Switch supports IGMP snooping, enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Three scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Table 148 Firmware Specifications

FEATURE	DESCRIPTION
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
IP Multicast	With IP multicast, the Switch delivers IP packets to a group of hosts on the network - not everybody. In addition, the Switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
RIP	RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers.
OSPF	OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information. OSPF is best suited for large networks.
DVMRP	DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol.
VRRP	Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authentication and Accounting	The Switch supports authentication and accounting services via RADIUS and TACACS+ AAA servers.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.

Table 148 Firmware Specifications

FEATURE	DESCRIPTION
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 149 Feature Specifications

Layer 2 Features	Bridging	16K MAC addresses Static MAC address filtering by source/destination Broadcast storm control Static MAC address forwarding
	Switching	Switching fabric: 48 Gbps, non-blocking Max. Frame size: 1522 bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
	STP	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Multiple Rapid Spanning Tree capability (4 configurable trees) IEEE 802.1s Multiple Spanning Tree Protocol
	QoS	IEEE 802.1p Eight priority queues per port Port-based egress traffic shaping Rule-based traffic mirroring Supports IGMP snooping
	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K, 1000 static maximum Supports GVRP Double tagging for VLAN stacking Protocol Based VLAN Subnet Based VLAN
	Port Aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Six groups (up to 8 ports each)
	Port mirroring	All ports support port mirroring Support port mirroring per IP/TCP/UDP
	Bandwidth control	Supports rate limiting at 64K increment

Table 149 Feature Specifications (continued)

Layer 3 Features	IP Capability	IPv4 support 64 IP routing domains 8K IP address table Wire speed IP forwarding
	Routing protocols	Unicast: RIP-V1/V2, OSPF V2 Multicast: DVMRP, IGMP V1/V2/V3 Static Routing VRRP
	IP services	DHCP relay; VLAN based DHCP server/relay DHCP Snooping
Security		IEEE 802.1x port-based authentication Static MAC address filtering Limiting number of dynamic addresses per port

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 150 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2131, RFC 2132	Dynamic Host Configuration Protocol (DHCP)
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2338	Virtual Router Redundancy Protocol (VRRP)
RFC 2698	Two Rate Three Color Marker (TRTCM)
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 3046	DHCP Relay

Table 150 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3ah	Ethernet OAM (Operations, Administration and Maintenance)
IEEE 802.3x	Flow Control
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

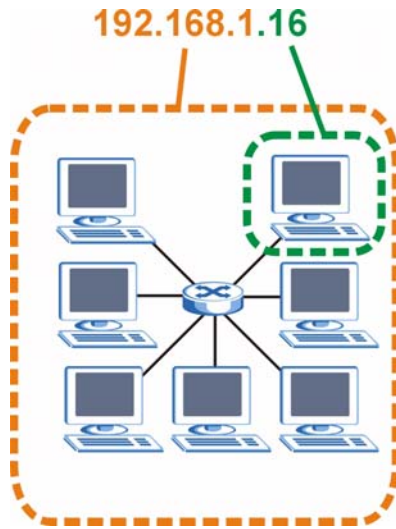
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 212 Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 151 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 152 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 153 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 154 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 154 Alternative Subnet Mask Notation (continued)

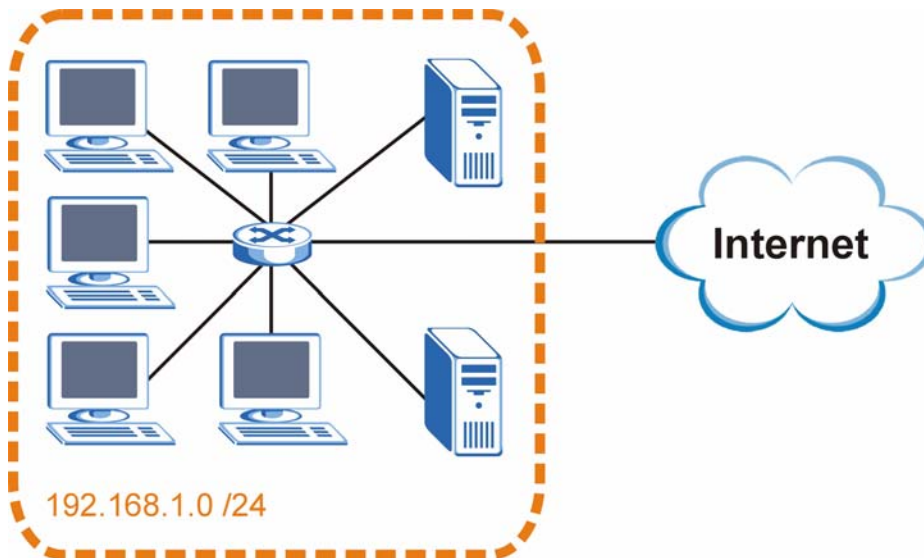
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

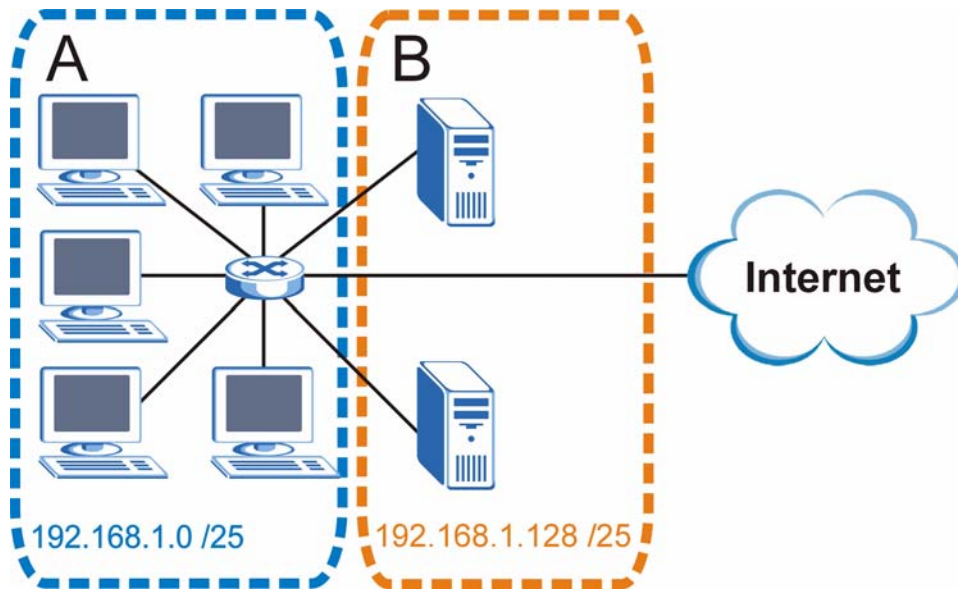
The following figure shows the company network before subnetting.

Figure 213 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 214 Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 155 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 156 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 157 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 158 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 159 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 159 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 160 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 161 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 161 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Switch.

Once you have decided on the network number, pick an IP address for your Switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

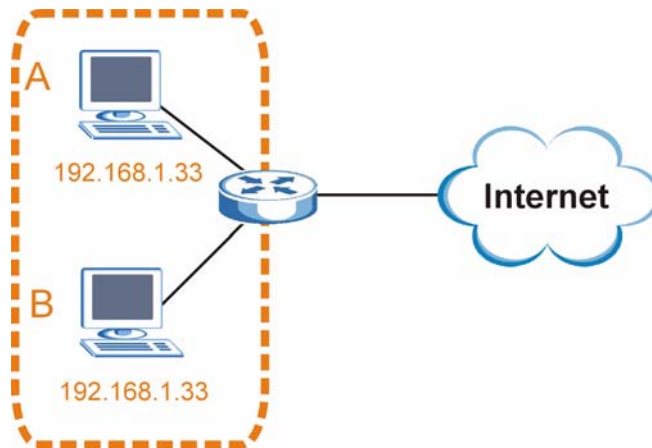
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

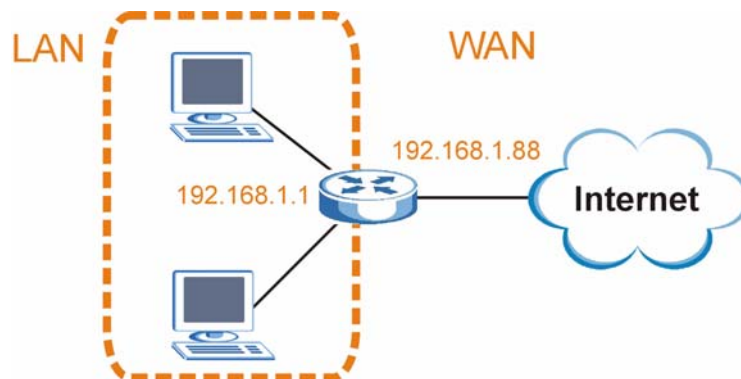
Figure 215 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

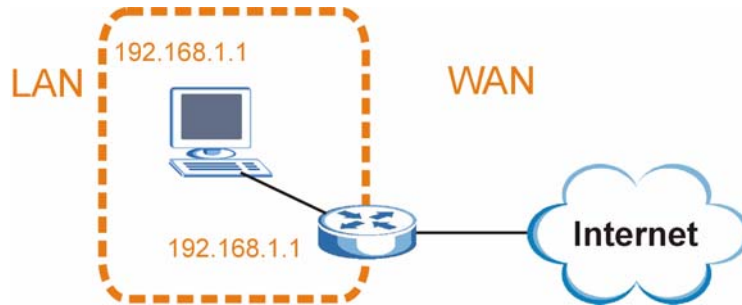
Figure 216 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 217 Conflicting Computer and Router IP Addresses Example



Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 162 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 162 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 162 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-690969
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave., Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: <ftp.us.zyxel.com>
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: [ftp.zyxel.co.uk](ftp://ftp.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK, Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

“+” is the (prefix) number you dial to make an international telephone call.

Index

Numerics

802.1P priority [87](#)

A

AAA [185](#)

AAA (Authentication, Authorization and Accounting) [185](#)

access control

limitations [285](#)

login account [294](#)

remote management [301](#)

service port [300](#)

SNMP [286](#)

accounting [185](#)

setup [190](#)

accounts

and modes [328](#)

address learning, MAC [99](#)

Address Resolution Protocol (ARP) [319](#), [323](#), [324](#)

administrator password [295](#)

age [123](#)

aggregator ID [135](#), [136](#)

aging time [82](#)

alternative subnet mask notation [433](#)

applications

backbone [37](#)

bridging [38](#)

IEEE 802.1Q VLAN [39](#)

switched workgroup [38](#)

Area Border Router (ABR) [229](#)

area ID

and OSPF [235](#)

ARP

how it works [319](#)

viewing [319](#)

ARP (Address Resolution Protocol) [319](#)

ARP inspection [199](#), [201](#)

and MAC filter [202](#)

configuring [202](#)

syslog messages [202](#)

trusted ports [202](#)

AS Boundary Router [229](#)

authentication [185](#), [235](#)

and OSPF [235](#)

setup [190](#)

Authentication, Authorization and Accounting, see
AAA [185](#)

authorization [185](#)

privilege levels [191](#)

automatic VLAN registration [92](#)

Autonomous System

and OSPF [229](#)

Autonomous System (AS) [229](#), [245](#)

B

back up, configuration file [282](#)

Backbone Router (BR) [229](#)

backbone, routing [229](#)

Backup Designated Router(BDR), and OSPF [230](#)

bandwidth control [127](#), [428](#)

egress rate [128](#)

ingress rate [128](#)

setup [127](#)

bandwidth control and TRTCM [255](#)

basic settings [77](#)

BDR (Backup Designated Router) [230](#)

binding [199](#)

binding table [199](#)

building [199](#)

BPDUs (Bridge Protocol Data Units) [110](#)

Bridge Protocol Data Units (BPDUs) [110](#)

bridging [428](#)

broadcast storm control [129](#)

C

certifications [445](#)

notices [446](#)

viewing [446](#)

CFI (Canonical Format Indicator) [91](#)

changing the password [61](#)

CIR (Committed Information Rate) [127](#)

CIST [114](#)

Class of Service (CoS) [251](#)

- classifier [151, 153](#)
 - and QoS [151](#)
 - editing [154](#)
 - example [155](#)
 - overview [151](#)
 - setup [151, 153, 154](#)
 - viewing [154](#)
- CLI
 - syntax conventions [326](#)
- cloning a port See port cloning
- cluster management [309](#)
 - and switch passwords [314](#)
 - cluster manager [309, 313](#)
 - cluster member [309, 314](#)
 - cluster member firmware upgrade [311](#)
 - network example [309](#)
 - setup [312](#)
 - specification [309](#)
 - status [310](#)
 - switch models [309](#)
 - VID [313](#)
 - web configurator [311](#)
- cluster manager [309](#)
- cluster member [309](#)
- Command Line Interface
 - introduction [325](#)
- Command Line Interface (CLI) [325](#)
- Command Line Interface, See also commands
 - accessing [325](#)
- commands [325](#)
 - accessing [325](#)
 - and configuration file [332](#)
 - and passwords [327](#)
 - configure tagged VLAN example [403](#)
 - exit [332](#)
 - forwarding process example [407](#)
 - getting help [329](#)
 - interface [395](#)
 - logging in [326](#)
 - modes [328](#)
 - modes summary [329](#)
 - static VLAN table example [407](#)
 - summary [332](#)
 - syntax conventions [326](#)
 - user mode details [333](#)
 - using history [331](#)
 - VLAN [403](#)
- Committed Information Rate (CIR) [127](#)
- Common and Internal Spanning Tree, See CIST [114](#)
- config mode [328](#)
 - examples [383](#)
- configuration [226](#)
 - change running config [281](#)
 - saving [331](#)
- configuration file [62, 332](#)
 - and commands [332](#)

- backup [282](#)
 - restore [62, 282](#)
 - saving [280](#)
- configuration, saving [61](#)
- console port
 - commands [325](#)
 - settings [46, 325](#)
- contact information [449](#)
- copying port settings, See port cloning
- copyright [445](#)
- CPU management port [101](#)
- current date [80](#)
- current time [80](#)
- customer support [449](#)

D

- Database Description (DD) [230](#)
- daylight saving time [80](#)
- default gateway [265](#)
- Designated Router(DR), and OSPF [230](#)
- DHCP [259](#)
 - client IP pool [265](#)
 - configuration options [259](#)
 - modes [259](#)
 - relay agent [259](#)
 - relay example [263](#)
 - server [259](#)
 - setup [264](#)
 - VLAN settings [264](#)
- DHCP (Dynamic Host Configuration Protocol) [259](#)
- DHCP relay option 82 [201](#)
- DHCP snooping [199](#)
 - configuring [201](#)
 - DHCP relay option 82 [201](#)
 - trusted ports [200](#)
 - untrusted ports [200](#)
- DHCP snooping database [200](#)
- diagnostics [303](#)
 - Ethernet port test [303](#)
 - ping [303](#)
 - system log [303](#)
- Differentiated Service (DiffServ) [251](#)
- DiffServ [251](#)
 - activate [254](#)
 - and TRTCM [254](#)
 - DS field [251](#)
 - DSCP [251](#)
 - DSCP-to-IEEE802.1p mapping [256](#)
 - network example [252](#)
 - PHB [251](#)
- dimensions [425](#)

disclaimer [445](#)
 double-tagged frames [165](#)
 DR (Designated Router) [230](#)
 DS (Differentiated Services) [251](#)
 DSCP
 DSCP-to-IEEE802.1p mapping [256](#)
 service level [251](#)
 what it does [251](#)
 DSCP (DiffServ Code Point) [251](#)
 DVMRP
 Autonomous System [245](#)
 default timer setting [248](#)
 error message [247](#)
 graft [246](#)
 how it works [245](#)
 implementation [245](#)
 probe [246](#)
 prune [246](#)
 report [246](#)
 setup [246](#)
 terminology [246](#)
 threshold [246](#)
 DVMRP (Distance Vector Multicast Routing Protocol) [245](#)
 dynamic link aggregation [133](#)

E

egress port [103](#)
 egress rate, and bandwidth control [128](#)
 enable mode [328](#)
 examples [377](#)
 Ethernet broadcast address [319](#)
 Ethernet port test [303](#)
 Ethernet ports
 default settings [46](#)
 external authentication server [186](#)

F

fan speed [78](#)
 FCC interference statement [445](#)
 feature summary [58](#)
 file transfer using FTP
 command example [283](#)
 filename convention, configuration
 configuration
 file names [283](#)
 filtering [107](#)

 rules [107](#)
 filtering database, MAC table [315](#)
 firmware [78](#)
 upgrade [281](#), [311](#)
 flow control [87](#)
 back pressure [87](#)
 IEEE802.3x [87](#)
 forwarding
 delay [123](#)
 frames
 tagged [97](#)
 untagged [97](#)
 front panel [45](#)
 FTP [283](#)
 file transfer procedure [283](#)
 restrictions over WAN [284](#)

G

GARP [92](#)
 GARP (Generic Attribute Registration Protocol) [92](#)
 GARP terminology [92](#)
 GARP timer [82](#), [92](#)
 general features [428](#)
 general setup [79](#)
 getting help [63](#)
 gigabit Ethernet ports [46](#)
 GMT (Greenwich Mean Time) [80](#)
 GVRP [92](#), [97](#)
 and port assignment [97](#)
 GVRP (GARP VLAN Registration Protocol) [92](#), [398](#)

H

hardware installation [41](#)
 hardware monitor [78](#)
 hardware overview [45](#)
 hello time [123](#)
 help
 in command interpreter [329](#)
 history
 in command interpreter [331](#)
 hops [123](#)
 HTTPS [297](#)
 certificates [297](#)
 implementation [297](#)
 public keys, private keys [297](#)
 HTTPS example [298](#)

humidity [425](#)

I

IANA [438](#)

IEEE 802.1p, priority [83](#)

IEEE 802.1x

activate [143](#), [144](#), [188](#), [190](#)

reauthentication [144](#)

IEEE 802.1x, port authentication [141](#)

IGMP [241](#), [245](#)

how it works [242](#)

port based [243](#)

setup [243](#)

version [171](#), [242](#)

version 3 [243](#)

IGMP (Internet Group Management Protocol) [171](#)

IGMP filtering [171](#)

profile [176](#)

profiles [173](#)

IGMP snooping [171](#)

and VLANs [172](#)

MVR [177](#)

setup [174](#)

ingress port [102](#)

ingress rate, and bandwidth control [128](#)

installation

freestanding [41](#)

precautions [42](#)

rack-mounting [42](#)

interface [232](#)

and OSPF [236](#)

interface commands [395](#)

interface, and OSPF [230](#)

Internal Router (IR) [229](#)

Internet Assigned Numbers Authority

See IANA [438](#)

introduction [37](#)

IP

capability [429](#)

interface [83](#), [269](#)

routing domain [83](#)

services [429](#)

setup [83](#)

IP multicast [241](#)

IP source guard [199](#)

ARP inspection [199](#), [201](#)

DHCP snooping [199](#)

static bindings [199](#)

IP table [317](#)

how it works [317](#)

L

LACP [133](#)

system priority [137](#)

timeout [138](#)

layer 2 features [428](#)

layer 3 features [429](#)

LEDs [51](#)

limit MAC address learning [148](#)

Link Aggregate Control Protocol (LACP) [133](#)

link aggregation [133](#)

dynamic [133](#)

ID information [134](#)

setup [135](#), [136](#)

status [134](#)

link state database [230](#), [232](#)

lockout [61](#)

log [303](#)

login [55](#)

password [61](#)

login account

Administrator [294](#)

non-administrator [295](#)

login accounts [294](#)

configuring via web configurator [294](#)

multiple [294](#)

number of [294](#)

login password [295](#)

loop guard [219](#)

examples [220](#)

port shut down [221](#)

setup [221](#)

vs STP [219](#)

LSA (Link State Advertisement) [230](#)

M

MAC (Media Access Control) [78](#)

MAC address [78](#), [319](#)

maximum number per port [148](#)

MAC address learning [82](#), [99](#), [105](#), [148](#)

specify limit [148](#)

MAC authentication [141](#)

aging time [145](#)

example [142](#)

setup [144](#)

MAC filter

and ARP inspection [202](#)

MAC table [315](#)

how it works [315](#)

viewing [316](#)

- maintenance
 - configuration backup [282](#)
 - firmware [281](#)
 - restoring configuration [282](#)
 - maintenance [279](#)
 - current configuration [279](#)
 - main screen [279](#)
 - Management Information Base (MIB) [286](#)
 - management port [103](#)
 - managementmanagement interface, See also CLI
 - man-in-the-middle attacks [201](#)
 - max
 - age [123](#)
 - hops [123](#)
 - metric [234](#)
 - MIB
 - and SNMP [286](#)
 - supported MIBs [287](#)
 - MIB (Management Information Base) [286](#)
 - mini GBIC ports [47](#)
 - connection speed [47](#)
 - connector type [47](#)
 - transceiver installation [47](#)
 - transceiver removal [48](#)
 - mirroring ports [131](#)
 - modes
 - and accounts [328](#)
 - in command interpreter [328](#)
 - monitor port [131](#), [132](#)
 - mounting brackets [42](#)
 - MRSTP
 - status [120](#)
 - MSA (MultiSource Agreement) [47](#)
 - MST ID [113](#)
 - MST Instance, See MSTI [113](#)
 - MST region [113](#)
 - MSTI [113](#)
 - MSTP [109](#), [112](#)
 - bridge ID [125](#), [126](#)
 - configuration [122](#)
 - configuration digest [126](#)
 - forwarding delay [123](#)
 - Hello Time [125](#)
 - hello time [123](#)
 - Max Age [125](#)
 - max age [123](#)
 - max hops [123](#)
 - path cost [124](#)
 - port priority [124](#)
 - revision level [123](#)
 - status [124](#)
 - MTU (Multi-Tenant Unit) [81](#)
 - multicast [171](#), [249](#)
 - 802.1 priority [173](#)
 - and IGMP [171](#)
 - and VLAN [249](#)
 - configuration [250](#)
 - IP addresses [171](#)
 - overview [171](#), [249](#)
 - setup [172](#), [173](#)
 - vs. unicast [249](#)
 - vs.broadcast [249](#)
 - multicast delivery tree [246](#)
 - multicast group [176](#)
 - multicast router ('mrouter') [246](#)
 - multicast VLAN [180](#)
 - Multiple Rapid Spanning Tree Protocol [111](#)
 - Multiple RSTP [111](#)
 - Multiple Spanning Tree Protocol, See MSTP [109](#), [112](#)
 - Multiple STP [112](#)
 - MVR [177](#)
 - configuration [178](#)
 - group configuration [180](#)
 - network example [177](#)
 - MVR (Multicast VLAN Registration) [177](#)
- N**
 - NAT [438](#)
 - network management system (NMS) [286](#)
 - no commands examples [387](#)
 - NTP (RFC-1305) [80](#)
- O**
 - OSPF [229](#)
 - advantages [229](#)
 - area [229](#), [235](#)
 - Area 0 [229](#)
 - area ID [235](#)
 - authentication [235](#)
 - autonomous system [229](#)
 - backbone [229](#)
 - configuration steps [231](#)
 - general settings [233](#)
 - how it works [230](#)
 - interface [230](#), [232](#), [236](#)
 - link state database [230](#), [232](#)
 - network example [230](#)
 - priority [230](#)
 - redistribute route [234](#)
 - route cost [236](#)
 - router elections [230](#)
 - router ID [234](#)

- router types [229](#)
- status [231](#)
- stub area [229](#), [236](#)
- virtual link [230](#)
- virtual links [238](#)
- vs RIP [229](#)
- OSPF (Open Shortest Path First) [229](#)

P

- password [61](#)
 - administrator [295](#)
- Peak Information Rate (PIR) [127](#)
- PHB (Per-Hop Behavior) [251](#)
- ping, test connection [303](#)
- PIR (Peak Information Rate) [127](#)
- policy [159](#), [160](#)
 - and classifier [159](#)
 - and DiffServ [157](#)
 - configuration [159](#)
 - example [161](#)
 - overview [157](#)
 - rules [157](#), [158](#)
 - viewing [160](#)
- policy configuration [160](#)
- port authentication [141](#)
 - and RADIUS [186](#)
 - IEEE802.1x [143](#), [188](#), [190](#)
 - MAC authentication [141](#)
- port based
 - IGMP [243](#)
- port based VLAN type [82](#)
- port cloning [323](#), [324](#)
 - advanced settings [323](#), [324](#)
 - basic settings [323](#), [324](#)
- port details [72](#)
- port isolation [97](#), [102](#)
- port mirroring [131](#), [132](#), [370](#), [428](#)
 - and commands [397](#)
 - direction [132](#)
 - egress [132](#)
 - ingress [132](#)
- port redundancy [133](#)
- port security [147](#)
 - limit MAC address learning [148](#)
 - MAC address learning [147](#)
 - overview [147](#)
 - setup [147](#), [221](#)
- port setup [85](#)
- port status [71](#)
- port VID
 - default for all ports [372](#)

- port VLAN trunking [93](#)
- port-based VLAN [100](#)
 - all connected [102](#)
 - port isolation [102](#)
 - settings wizard [102](#)
- ports
 - “standby” [133](#)
 - diagnostics [303](#)
 - mirroring [131](#)
 - speed/duplex [86](#)
- power
 - backup power supply connector [51](#)
 - voltage [79](#)
- power module
 - current rating [50](#)
 - power wire [50](#)
- power specification [425](#)
- power status [79](#)
- priority level [83](#)
- priority, and OSPF [231](#)
- priority, queue assignment [83](#)
- product registration [447](#)
- protocol based VLAN
 - hexadecimal notation for protocols [99](#)
 - priority [99](#)
- PVID [91](#), [97](#)
- PVID (Priority Frame) [91](#)

Q

- QoS [428](#)
 - and classifier [151](#)
- Queue priority [164](#)
- Queue weight [164](#)
- queue weight [163](#)
- queuing [163](#)
 - SPQ [163](#)
 - WRR [163](#)
- Queuing algorithm [164](#)
- Queuing method [164](#)
- queuing method [163](#)

R

- RADIUS [185](#), [186](#)
 - advantages [186](#)
 - and port authentication [186](#)
 - and tunnel protocol attribute [194](#)
 - Network example [185](#)

- server [186](#)
- settings [186](#)
- setup [186](#)
- Rapid Spanning Tree Protocol, See RSTP. [109](#)
- rear panel [48](#)
- reboot
 - load configuration [281](#)
- reboot system [281](#)
- redistribute route [234](#)
- registration
 - product [447](#)
- related documentation [3](#)
- remote management [301](#)
 - service [302](#)
 - trusted computers [301](#)
- resetting [62, 280](#)
 - to factory default settings [280](#)
- restoring configuration [62, 282](#)
- Reverse Path Forwarding (RPF) [246](#)
- Reverse Path Multicasting (RPM) [245](#)
- RFC 3164 [305](#)
- RIP
 - configuration [227](#)
 - direction [227](#)
 - overview [227](#)
 - version [227](#)
 - vs OSPF [229](#)
- RIP (Routing Information Protocol) [227](#)
- Round Robin Scheduling [163](#)
- router ID [234](#)
- routing domain [83, 269](#)
- routing protocols [234, 429](#)
- routing table [321](#)
- RSTP [109](#)
- rubber feet [41](#)

S

- safety certifications [430](#)
- safety warnings [6](#)
- save configuration [61, 280](#)
- screen summary [58](#)
- Secure Shell See SSH
- security [429](#)
- service access control [300](#)
 - service port [301](#)
- SFP (Small Form-factor Pluggable) [47](#)
- show commands
 - examples [377](#)
- Simple Network Management Protocol, see SNMP

- SNMP [286](#)
 - agent [286](#)
 - and MIB [286](#)
 - and security [287](#)
 - authentication [293](#)
 - communities [292](#)
 - management model [286](#)
 - manager [286](#)
 - MIB [287](#)
 - network components [286](#)
 - object variables [286](#)
 - protocol operations [286](#)
 - security [293](#)
 - setup [291, 293](#)
 - version 3 [287](#)
 - versions supported [286](#)
- SNMP traps [287, 288, 289, 290, 291](#)
 - setup [293](#)
- Spanning Tree Protocol, See STP. [109](#)
- SPQ (Strict Priority Queuing) [163](#)
- SSH
 - encryption methods [297](#)
 - how it works [296](#)
 - implementation [297](#)
- SSH (Secure Shell) [296](#)
- SSL (Secure Socket Layer) [297](#)
- standby ports [133](#)
- static bindings [199](#)
- static link aggregation example [138](#)
- static MAC address [105](#)
- static MAC forwarding [99, 105](#)
- static routes [225, 226](#)
- static trunking example [138](#)
- Static VLAN [95](#)
- static VLAN
 - control [96](#)
 - tagging [96](#)
- status [56, 71](#)
 - LED [51](#)
 - link aggregation [134](#)
 - MSTP [124](#)
 - OSPF [231](#)
 - port [71](#)
 - port details [72](#)
 - power [79](#)
 - STP [117, 120](#)
 - VLAN [94](#)
 - VRRP [268](#)
- STP [109, 428](#)
 - bridge ID [118, 121](#)
 - bridge priority [116, 119](#)
 - configuration [116, 119](#)
 - designated bridge [110](#)
 - forwarding delay [117, 120](#)
 - Hello BPDU [110](#)
 - Hello Time [117, 118, 119, 121](#)

- how it works [110](#)
- Max Age [117](#), [118](#), [120](#), [121](#)
- path cost [110](#), [117](#), [120](#)
- port priority [117](#), [120](#)
- port state [111](#)
- root port [110](#)
- status [117](#), [120](#)
- terminology [109](#)
- vs loop guard [219](#)
- stub area [229](#), [236](#)
- stub area, See also OSPF [236](#)
- subnet [431](#)
- subnet based VLAN
 - and DHCP VLAN [99](#)
 - setup [99](#)
- subnet based VLANs [98](#)
- subnet mask [432](#)
- subnetting [434](#)
- switch lockout [61](#)
- switch reset [62](#)
- switch setup [81](#)
- switching [428](#)
- syntax conventions [4](#)
- syslog [202](#), [305](#)
 - protocol [305](#)
 - server setup [306](#)
 - settings [305](#)
 - setup [305](#)
 - severity levels [305](#)
- system information [77](#)
- system log [303](#)
- system reboot [281](#)

T

- TACACS+ [185](#), [186](#)
 - setup [188](#)
- TACACS+ (Terminal Access Controller Access-Control System Plus) [185](#)
- tagged VLAN [91](#)
- Telnet
 - commands [326](#)
 - logging in [326](#)
 - management [326](#)
- temperature [425](#)
- temperature indicator [78](#)
- time
 - current [80](#)
 - time zone [80](#)
- Time (RFC-868) [80](#)
- time server [80](#)

- time service protocol [80](#)
 - format [80](#)
- Time To Live (TTL) [246](#)
- trademarks [445](#)
- transceiver
 - installation [47](#)
 - removal [48](#)
- traps
 - destination [292](#)
- TRTCM
 - and bandwidth control [255](#)
 - and DiffServ [254](#)
 - color-aware mode [253](#)
 - color-blind mode [253](#)
 - setup [255](#)
- TRTCM (Two Rate Three Color Marker) [252](#)
- trunk group [133](#)
- trunking [133](#), [428](#)
 - example [138](#)
- trusted ports
 - ARP inspection [202](#)
 - DHCP snooping [200](#)
- tunnel protocol attribute, and RADIUS [194](#)
- turn on the power [51](#)
- Two Rate Three Color Marker (TRTCM) [252](#)
- Type of Service (ToS) [251](#)

U

- untrusted ports
 - ARP inspection [202](#)
 - DHCP snooping [200](#)
- user mode [328](#)
 - examples [377](#)
- user profiles [185](#)

V

- Vendor Specific Attribute See VSA
- ventilation [42](#)
- ventilation holes [42](#)
- VID [85](#), [91](#), [94](#), [95](#), [167](#)
 - number of possible VIDs [91](#)
 - priority frame [91](#)
- VID (VLAN Identifier) [91](#)
- virtual links [238](#)
- virtual links, and OSPF [230](#)
- Virtual Router
 - status [268](#)

Virtual Router (VR) [267](#)
Virtual Router Redundancy Protocol (VRRP) [267](#)
VLAN [81, 91, 428](#)
 acceptable frame type [97](#)
 and DHCP [264](#)
 automatic registration [92](#)
 ID [91](#)
 IGMP snooping [172](#)
 ingress filtering [97](#)
 introduction [81](#)
 number of VLANs [94](#)
 port isolation [97](#)
 port number [95](#)
 port settings [96](#)
 port-based VLAN [100](#)
 port-based, all connected [102](#)
 port-based, isolation [102](#)
 port-based, wizard [102](#)
 static VLAN [95](#)
 status [94, 95](#)
 subnet based [98](#)
 tagged [91](#)
 trunking [93, 98](#)
 type [82, 93](#)
VLAN (Virtual Local Area Network) [81](#)
VLAN commands examples [403](#)
VLAN number [85](#)
VLAN stacking [165, 167](#)
 configuration [168](#)
 example [165](#)
 frame format [167](#)
 port roles [166, 169](#)
 priority [167](#)
VRID (Virtual Router ID) [268](#)
VRRP [267](#)
 advertisement interval [270](#)
 authentication [270](#)
 backup router [267](#)
 configuration example [272](#)
 Hello message [270](#)
 how it works [267](#)
 interface setup [269](#)
 master router [267](#)
 network example [267, 272](#)
 parameters [270](#)
 preempt mode [270, 271](#)
 priority [270, 271](#)
 status [268](#)
 uplink gateway [271](#)
 uplink status [268](#)
 Virtual Router [267](#)
 Virtual Router ID [271](#)
 VRID [268](#)
VSA [193](#)

W

warranty [446](#)
 note [447](#)
web configurator [55](#)
 getting help [63](#)
 home [56](#)
 login [55](#)
 logout [63](#)
 navigation panel [57](#)
 screen summary [58](#)
weight, queuing [163](#)
Weighted Round Robin Scheduling (WRR) [163](#)
WRR (Weighted Round Robin Scheduling) [163](#)

Z

ZyNOS (ZyXEL Network Operating System) [283](#)

